Desarrollo de un Plan Director de Seguridad para la implementación de un SGSI basado en la norma ISO/IEC 27001

TRABAJO FINAL DE MÁSTER

Autor: Beatriz Molina Cañamero

Tutor: Antonio José Segovia Henares

Fecha: diciembre 2018

MÁSTER INTERUNIVERSITARIO EN SEGURIDAD DE LA TECNOLOGÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES (MISTIC)

Resumen

En el presente trabajo se van a dar las pautas para poder llevar a cabo la implantación de un Plan de Seguridad de la Información para la implantación de un Sistema de Gestión de Seguridad de la Información de una determinada empresa que quiere gestionar de forma eficaz la seguridad, tomando como referencia la norma internacional ISO 27001:2015 y los controles de seguridad de la norma Internacional ISO/IEC 27002:2013.

Palabras clave

Seguridad de la Información, Seguridad Informática, Análisis de Riesgos, Gestión de Riesgos, ISO / IEC 27001, ISO/IEC 27002, SGSI.

Abstract

In this Project will be given a guidelines to carry out an Information Security Plan for the implementation of an Information Security Management System of a company that wants a effective security management, taking as reference the standard ISO 27001:2015 and the security controls of the standard ISO/ IEC 27002:2013.

Keywords

Information Security, IT Security, Risk Analysis, Risk Management, ISO / IEC 27001, ISO / IEC 27002, information management, ISMS.

ÍNDICE DE CONTENIDOS

1. INTRODUCCIÓN

En el presente trabajo se van a dar las pautas para poder llevar a cabo el desarrollo de un Plan Director de Seguridad de la Información para la implementación de un Sistema de Gestión de Seguridad de la Información en una determinada organización, pero que se puede extrapolar a otras organizaciones particularizando ciertos aspectos, basándose en una norma de referencia internacional, la ISO/IEC 27001:2015.

Primero, se hará un Análisis Diferencial del cumplimiento de la empresa con respecto a la norma ISO/IEC 27001:2015 y los controles que aparecen en la norma ISO/IEC 27002:2013. Después, se procederá a realizar un Análisis de Riesgos donde se analizará el inventario de activos de la organización, se identificarán las vulnerabilidades y posibles amenazas a los que están expuestos dichos activos, y el impacto potencial que pueden causar.

Segundo, se propondrá un Plan de Proyectos de Mejora para hacerle frente a esas amenazas y vulnerabilidades encontradas, proponiendo proyectos y salvaguardas para implementar un grado de seguridad de la información razonable, y se hará hincapié en la protección de los principales sistemas de información y elementos que componen la red corporativa, los cuales dan soporte a actividades, servicios o procesos de negocio críticos dentro de la organización.

La Norma mencionada anteriormente, la ISO/IEC 27001, define los requisitos para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI), y se puede aplicar a organizaciones de índole variada. En ella se recogen los componentes que forman el sistema, la documentación mínima si se quiere certificar, los registros que permiten evidenciar el funcionamiento del sistema, y expone los controles y recomendaciones de seguridad anexados en una norma o guía de buenas prácticas, la ISO/IEC 27002.

Por tanto, para este proyecto se tomarán dichas normas en la que se basan miles de organizaciones actualmente para garantizar la seguridad de la información que tratan, y que sirven para gestionarla de una manera adecuada. Implantar un SGSI en la organización le va a permitir averiguar, gestionar y minimizar los posibles riesgos que atenten contra la seguridad de la información de su organización, asegurando la integridad, confidencialidad y disponibilidad, los tres pilares básicos de la seguridad de la información.

1.1 CONTEXTO Y JUSTIFICACIÓN

Hoy en día, se producen innumerables ataques informáticos de todo tipo en el mundo, algunos de los más peligrosos aprovechando vulnerabilidades tipo *zero-day* como es el caso del *ransomware* que afectó a multitud de organizaciones alrededor del mundo en Mayo del 2017 [1], usando como vector de ataque principal un correo spam que incluía un adjunto que al abrirlo, el exploit contenido en él, aprovechaba la vulnerabilidad para instalar el *ransomware* en el ordenador y además propagarse por los sistemas que estaban conectados a esa misma red cifrando gran cantidad de datos, y por tanto bloqueando el acceso a ellos.

Para protegernos y hacer frente a dichos ataques, y en general para mantener seguros los sistemas de posibles amenazas, nace el concepto de Seguridad de la Información, que se puede definir como el conjunto de prácticas y características que garantizan la confidencialidad, disponibilidad e integridad de la información que se procesa y almacena, labor que cada vez más empresas españolas están teniendo en cuenta, aunque todavía sigue siendo una opción considerada la mayor parte de las veces una vez causado el daño.

La rápida digitalización de los negocios, hace que las organizaciones inviertan cada vez más en ciberseguridad en España y en todo el mundo, ya que, según un estudio desarrollado durante el 2016, las empresas españolas pierden, de media, 1,32 millones de euros al año como consecuencia de los ataques informáticos o ciberataques, poniendo de manifiesto que cientos de ellas son vulnerables. Es por ello, que desde el año 2012 el presupuesto medio de las empresas que invierten en ciberseguridad ha aumentado considerablemente, obteniendo como resultado un menor número de incidentes de seguridad, ya que se encuentran mejor preparadas y protegidas [2].

La información y los sistemas que la albergan pueden considerarse uno de los activos más valiosos que tiene una empresa, y su adecuada gestión y protección es crítica para asegurar la operativa de negocio frente ataques o desastres, además de para evitar daños reputacionales y como consecuencia tener grandes pérdidas, o librarse de penas sancionadoras por incumplimiento normativo. Debido a la gran importancia que tiene proteger los sistemas de información, existen diversas normas para la seguridad de la información. A continuación, se exponen las principales:

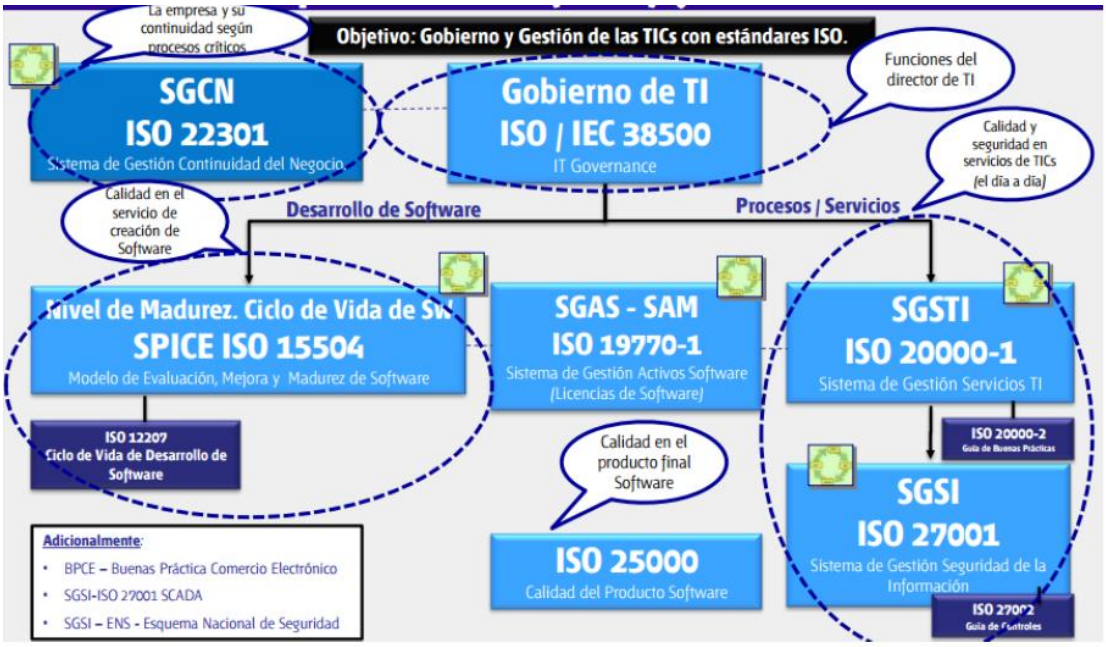

Fig. 1: Estándares ISO fuente: AENOR

Para garantizar la seguridad de la información se puede implantar un Sistema de Gestión de Seguridad de la Información, lo que va a permitir a la empresa:

- Analizar toda la estructura de sus sistemas de información.
- Facilitar la definición de procedimientos de trabajo para mantener su seguridad.
- Disponer de controles que permitan medir la eficacia de las medidas adoptadas y las que se vayan adoptando.
- Protegerse frente a riesgos que puedan amenazar el correcto funcionamiento de su negocio.

1.2 CONOCIENDO LA ISO/IEC 27002

Es difícil tomar un marco de referencia común de medidas de seguridad de la información válido para todas las organizaciones, ya que la seguridad de una empresa puede ser muy distinta dependiendo del campo específico en el que se halle enmarcada su principal función laboral, ya sea el comercial, industrial, bancario, asegurador, administrativo, etc. En este trabajo, se implantará la ISO/IEC 27001:2015 apoyándose en los controles de seguridad de la información descritos en la Norma Internacional ISO/IEC 27002:2013.

Para conocer grosso modo la ISO/IEC 27002, se describe a sí misma como *"los controles que guían la gestión de la seguridad de la información siendo aplicables a la mayoría de las organizaciones, convirtiéndose en un punto de partida para desarrollar unas directrices específicas para la organización"* [3].

Dichos controles complementan la norma de seguridad de la información ISO/IEC 27001, la cual está diseñada para *"proporcionar los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información"* [4], siguiendo el ciclo de Planificar-Hacer-Verificar-Actuar, mejor conocido como *Plan-Do-Check-Act.*

Fig. 2: Ciclo PDCA. Elaboración propia basándome en la descripción de dicha Norma

Cada uno de los 14 dominios tienen asociados uno o varios objetivos de seguridad sumando un total de 35 objetivos, y dentro de cada objetivo, uno o más controles de seguridad cuya implantación debe traducirse en la consecución del objetivo asociado sumando un total de 114 controles.

2. SITUACIÓN ACTUAL

2.1 DESCRIPCIÓN DE LA ORGANIZACIÓN

La organización bajo estudio y sobre la que se va a implantar el Plan Director de Seguridad, es una empresa aseguradora ubicada en Brasil, cuya Sede Central se ubica en España, y cuya principal actividad comercial se centra en la venta de pólizas de seguros con el debido servicio de gestión de asistencias.

Existen dos edificios ubicados en un mismo recinto. El primer edificio cuenta con dos plantas. En la primera planta se encuentran aproximadamente 70 empleados divididos en diferentes áreas que son: área técnica, comercial y marketing, operaciones, financiera, recursos humanos y legal; y en la planta baja existe una sala con el CPD, donde se encuentran todos los servidores, elementos de red y equipos de telecomunicaciones en general. Esta sala está protegida con sistemas de detección contra incendios, extintores y sistemas de climatización.

En el segundo edificio, se encuentra un call center que trabaja 24x7, con aproximadamente 100 puestos, los cuales, prestan más de 250.000 asistencias al año. Actualmente, la empresa está creciendo y se teme una degradación en dicho servicio.

Además, ambos edificios están conectados a grupos electrógenos que alimentan a los sistemas de energía ininterrumpida que serán usados en caso de apagones o si se produce algún incidente eléctrico.

El control de accesos al recinto tiene un cubículo con un guarda de seguridad privada 24x7, y tornos por donde se tiene que pasar una tarjeta de identificación. Además, en cada edificio existe una persona de recepción que se encarga de identificar a la persona que entra en él.

En cuanto al alcance de la organización con respecto a los sistemas de información que dan soporte a sus actividades, servicios y procesos de negocio, ésta cuenta con lo que a continuación se presenta para realizar su operativa del día a día:

- Disponen de servicios públicos accesibles desde Internet, ya que se pretende que empleados, clientes y usuarios remotos tengan acceso a ciertos servicios sin entrar a la red interna.

- Servidor Web conectado con red interna (Portal Web de la empresa): muestra información del servicio que presta la empresa, los sitios donde tiene presencia, lo que se puede contratar, y tiene conexión con bases de datos que se encuentran en la zona interna.

- Servicio de transferencia de ficheros a través del protocolo SFTP.

- Servicio de correo electrónico corporativo para hacer comunicaciones.

- Dentro de la red interna, se cuenta con distintos tipos de servidores internos tales como el controlador de dominio, distintas bases de datos de las que disponen, servidores de aplicaciones y consolas de gestión de seguridad de red.

Se ha nombrado desde la Sede Central un nuevo Responsable de Seguridad de la Información en la entidad brasileña, para mejorar la seguridad de la información de la organización y ayudar a implementar un SGSI junto con una consultora externa y el apoyo de la Dirección. Las principales motivaciones para llevarlo a cabo han sido:

- Temor al posible deterioro del servicio de call center debido al crecimiento de negocio y falta de personal. Ya ha sufrido indisponibilidad en alguna ocasión, se acumulan llamadas en espera, se cae el servicio y deja de estar disponible, además se añade que falta espacio en el edificio donde se encuentran. Esto provocaría el empeoramiento de la atención a los clientes.

- Entrada en vigor de nueva Ley en Brasil de Protección de Datos, y adaptación de la organización a ella.

- Temor a la indisponibilidad de los servicios y sistemas que se alojan en el CPD.

- Temor por la falta de protección de su activo clave, la información, ya que no se hace una comprobación del estado en el que se está, no siendo capaces de determinar si se está garantizando los pilares de la información que manejan: confidencialidad, integridad y disponibilidad, autenticidad y trazabilidad.

Como descripción de la estructura de la organización[1], se muestra un organigrama funcional con la jerarquía de la misma:

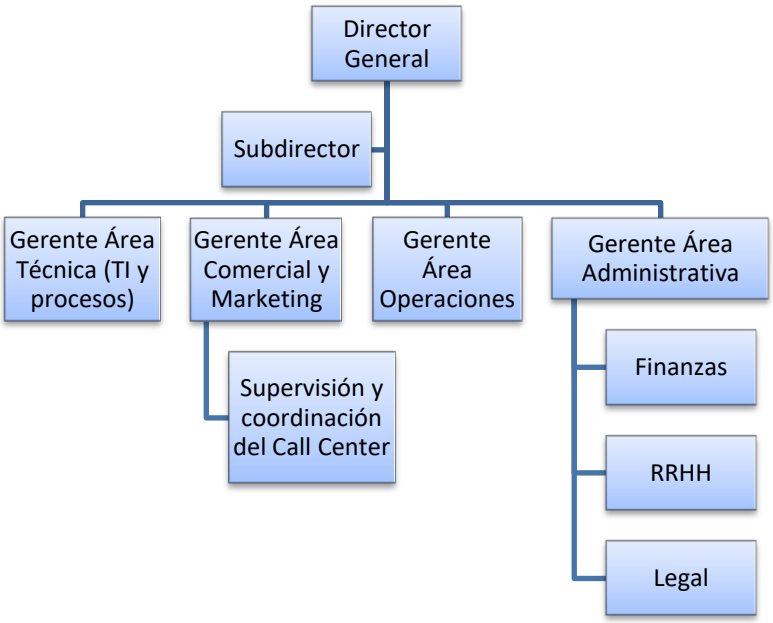

Fig.3: Organigrama de la empresa

[1] La figura de Responsable de la Seguridad de la Información estaría transversal a todas las áreas, y a un nivel de comunicación cercano a la Subdirección y la Dirección General.

Adicionalmente, se adjunta un diagrama de la arquitectura de red de la organización:

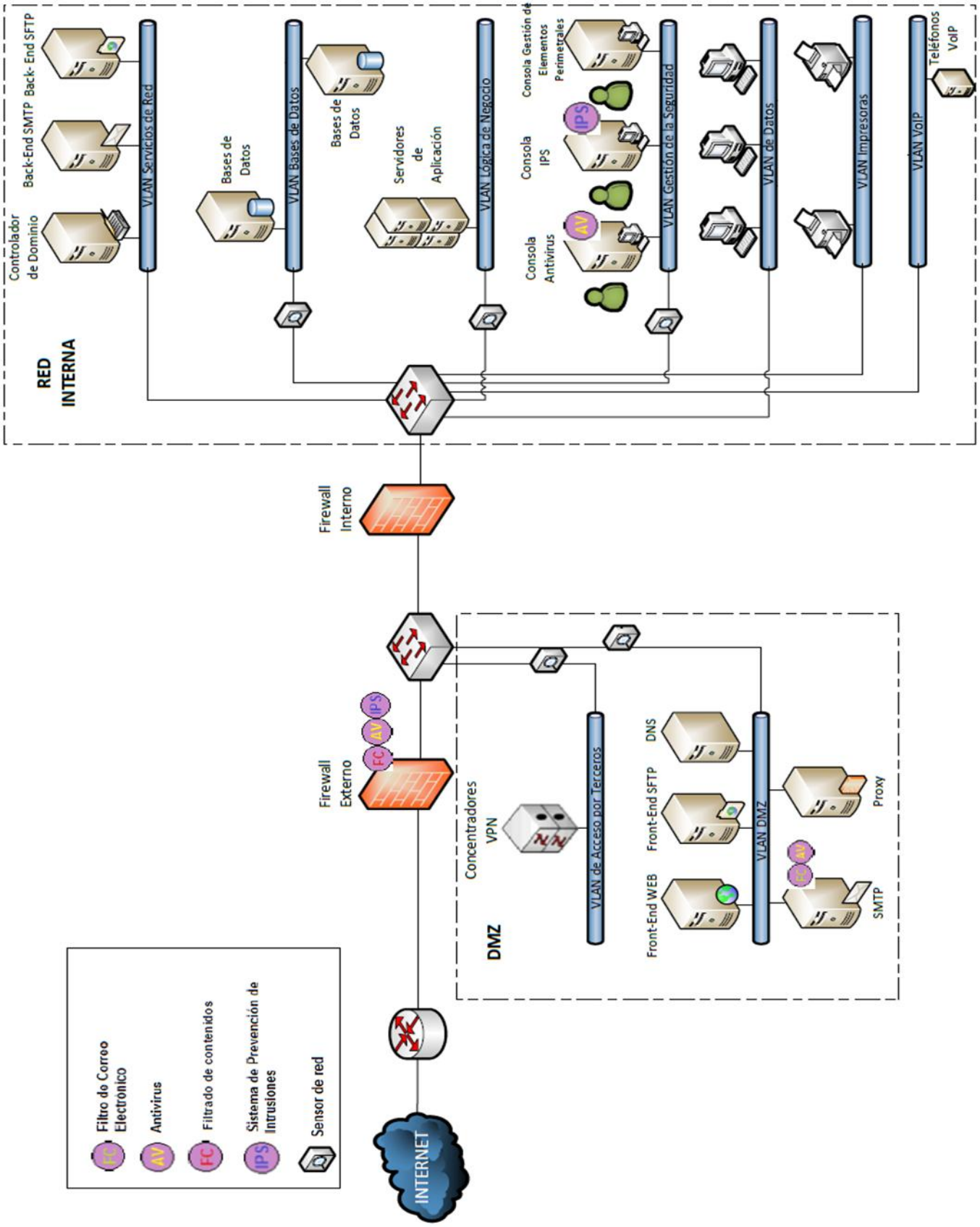

Fig. 4: Diagrama de red de la empresa (elaboración propia con Visio)

2.2 OBJETIVOS DEL PLAN DIRECTOR

Este proyecto tiene como objetivo hacer un profundo análisis de los sistemas de información de la empresa objeto para la elaboración de un Plan Director de Seguridad e implementación de un SGSI que ayude a establecer unas directrices de actuación para los aspectos organizativos, normativos, tecnológicos y de negocio, y así:

- Establecer unos niveles de seguridad adecuados a través de acciones realistas y alcanzables para mejorar el estado actual de los aspectos de seguridad de la información que tiene la organización.

- Dar respuesta a los crecientes riesgos y amenazas al negocio derivados de las posibles debilidades en la protección de su información.

- Evaluar el estado de la organización en materia de seguridad de la información y establecer medidas para su adecuada gestión y mejora.

- Dar mayor confianza a los clientes, los cuales requieran el cumplimiento de una serie de buenas prácticas en esta materia.

Estos objetivos ayudarán a determinar el alcance de dicho Plan Director de Seguridad.

2.3 ANÁLISIS DIFERENCIAL

Para saber el grado de adecuación de la organización con respecto a la norma ISO 27001:2015 y a los controles definidos en la ISO/IEC 27002:2013, se ha elaborado un análisis inicial o diferencial del estado de la organización.

A continuación, se presentan los resultados mostrando el porcentaje de cumplimiento que tiene la organización con respecto a los requisitos de la norma ISO 27001 y con respecto a cada control de la ISO 27002.

2.3.1 ANALISIS DIFERENCIAL RESPECTO A LA ISO 27001

La organización va a comenzar a implantar el Sistema de Gestión de la Seguridad de la Información desde cero, por eso no cumple con la mayoría de los requisitos establecidos en la norma ISO 27001.

REQUISITOS	COMENTARIOS	NIVEL DE CUMPLIMIENTO CON ISO 27001
4. CONTEXTO DE LA ORGANIZACIÓN		**13%**
4.1 Compresión de la organización y de su contexto	La organización es conocedora de su estructura y del negocio que gestionan, pero deben analizar la evolución del contexto donde se mueven y la importancia que tiene la seguridad de la información dentro de sus procesos para gestionar correctamente los riesgos y que la implantación del SGSI logre los resultados que se esperan.	50%
4.2 Comprensión de las necesidades y expectativas de las partes interesadas		0%
4.3 Determinación del alcance del sistema de gestión de la seguridad de la información		0%
4.4 Sistema de gestión de la seguridad de la información		0%
5. LIDERAZGO		**60%**
5.1 Liderazgo y compromiso	La Dirección de la organización ha aprobado el proyecto para la implementación de un SGSI basado en la norma ISO 27001 y se ha comprometido a dirigir y apoyar a las partes involucradas para contribuir a la eficacia del SGSI.	50%

5.2 Política	Disponen de una Política de Seguridad de la Información, la cual está aprobada por la Dirección, comunicada y publicada en la intranet local accesible para todos los empleados.	100%
5.3 Roles, responsabilidades y autoridades en la organización	La organización cuenta con un Comité de Seguridad que está constituido por una persona de Dirección y varios responsables, con los roles y sus responsabilidades asignadas, pero pendiente de formalizar por parte de la Dirección General y nunca se ha celebrado uno.	30%
6. PLANIFICACIÓN		**0%**
6.1 Acciones para tratar los riesgos y oportunidades		0%
6.2 Objetivos de seguridad de la información y planificación para su consecución		0%
7. SOPORTE		**30%**
7.1 Recursos	La Dirección ha destinado presupuesto para el establecimiento, implementación, mantenimiento y mejora del SGSI.	100%
7.2 Competencia		0%
7.3 Concienciación	Los empleados son conscientes de la existencia de la Política de la Seguridad de la Información de la organización	50%
7.4 Comunicación		0%
7.5 Información documentada		0%

8. OPERACIÓN		**0%**
8.1 Planificación y control operacional		0%
8.2 Apreciación de los riesgos de seguridad de la información		0%
8.3 Tratamiento de los riesgos de seguridad de la información		0%
9. EVALUACIÓN DEL DESEMPEÑO		**13%**
9.1 Seguimiento, medición, análisis y evaluación	Hasta el momento, se ha hecho seguimiento de algunos indicadores de la herramienta de gestión de inventario para ver el estado en materia de seguridad de la información.	40%
9.2 Auditoría interna	No se han llevado auditorías internas relativas a un SGSI.	0%
9.3 Revisión por la dirección		0%
10. MEJORA		**15%**
10.1 No conformidad y acciones correctivas	Se han llevado algunas acciones correctivas determinadas cuando ha habido incidencias en la organización.	30%
10.2 Mejora continua		0%

2.3.2 ANALISIS DIFERENCIAL RESPECTO A LA ISO 27002

CONTROLES	ANÁLISIS DIFERENCIAL RESPECTO CONTROLES ISO 27002	GRADO DE CONVERGENCIA ISO 27002
5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN		**50%**
5.1 Directrices de gestión de la seguridad de la información		
5.1.1 Políticas para la seguridad de la información	Disponen de una Política de Seguridad de la Información, la cual está aprobada por la Dirección, comunicada y publicada en la intranet local accesible para todos los empleados.	100%
5.1.2 Revisión de las políticas para la seguridad de la información	La Política de Seguridad de la Información no se ha revisado desde que se publicó hace dos años, y por tanto tampoco se ha creado un registro de actualizaciones de la misma.	0%
6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		**38%**
6.1 Organización interna		
6.1.1 Roles y responsabilidades en seguridad de la información	El Comité de Seguridad está constituido por un miembro de la Dirección, un Responsable de Seguridad de la Información y varias individuos a los cuales se les ha asignado unos roles y responsabilidades de seguridad asociadas, pero aún está pendiente de formalizar por parte de la Dirección y nunca se ha celebrado uno.	50%

6.1.2 Segregación de tareas	La segregación de funciones no se encuentra definida formalmente dentro de negocio, aunque existe un perfilado básico para diferenciar al personal de call center del personal de administración autorizado para acceder a determinados activos. Por otro lado, en cuanto a las funciones y responsabilidades asignadas para la implantación del SGSI, se deben aprobar y volver a revisar de cara a la implantación del SGSI. Actualmente, no se realiza ningún tipo de revisión o mantenimiento periódico de las funciones segregadas y las responsabilidades asociadas.	50%
6.1.3 Contacto con las autoridades	En la intranet hay publicado un documento explicando cómo comunicar un posible incidente de seguridad que se haya podido dar, y cómo actuar y a quién llamar en caso de emergencias.	85%
6.1.4 Contacto con grupos de interés especial	Se mantiene contacto con algunos grupos de interés especial (grupos legales de protección de datos de carácter personal por ejemplo), pero se tiene que tener contacto con otros grupos para estar actualizado en otras materias relativas a seguridad de la información.	60%
6.1.5 Seguridad de la información en la gestión de proyectos	La seguridad no está debidamente integrada dentro de los proyectos que surgen.	10%
6.2 Los dispositivos móviles y el teletrabajo		
6.2.1 Política de dispositivos móviles	No existe una política de dispositivos móviles dentro de la organización. Los dispositivos móviles principales que utilizan son los portátiles, los cuales no se encuentran cifrados, ni se hacen backups de la información que contienen.	10%
6.2.2 Teletrabajo	N/A. La organización no usa esta modalidad de trabajo.	0%

7. SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS		**53%**
7.1 Antes del empleo		
7.1.1 Investigación de antecedentes	RRHH suele revisar la veracidad de los datos y referencias aportadas teniendo en cuenta la ley aplicable, pidiendo las titulaciones del empleado y recomendaciones de anteriores empresas, pero no hay definido ningún procedimiento formal.	60%
7.1.2 Términos y condiciones del empleo	El empleado cuando va a firmar el contrato, acepta y firma la cláusula de confidencialidad y acepta los términos que le aplican relativos a la seguridad de la información.	80%
7.2 Durante el empleo		
7.2.1 Responsabilidades de gestión	Todos los empleados conocen la política de seguridad de la información, pero algunos departamentos desconocen exactamente cuáles son las responsabilidades que les son asignadas y los procedimientos que se deben llevar a cabo.	75%
7.2.2 Concienciación, educación y capacitación en seguridad de la información	No existe un plan de concienciación y formación de seguridad de la información acorde al puesto de trabajo para el personal. Lo único que tienen al respecto son emails que el departamento de TI manda de vez en cuando con consejos sobre seguridad.	30%
7.2.3 Proceso disciplinario	No está definido un proceso disciplinario, aunque existen algunas pautas fijadas por la Dirección cuando alguien provoca una brecha de seguridad. Los trabajadores conocen la Política de Seguridad de la Información, pero no son conscientes de qué pasaría si cometen alguna violación de las políticas o normativas de seguridad.	20%
7.3 Finalización del empleo o cambio en el puesto de trabajo		

7.3.1 Responsabilidades ante la finalización o cambio	Está definido un proceso de finalización de la relación con la organización o de cambio de puesto de trabajo, pero en este último caso, es posible que se sumen permisos al hacer cambios de situación del empleado dentro de la empresa.	50%
8. GESTIÓN DE ACTIVOS		**67%**
8.1 Responsabilidad sobre los activos		
8.1.1 Inventario de activos	Hay un inventario de activos gestionado por una herramienta de gestión de inventario que da información detallada de cada equipo. Dicha herramienta está instalada en los sistemas y da información detallada y actualizada del estado del mismo.	90%
8.1.2 Propiedad de los activos	Los activos que entran dentro del alcance del SGSI de la organización tienen asignados un propietario.	90%
8.1.3 Uso aceptable de los activos	Existe un procedimiento de uso aceptable de los activos publicado recientemente en la intranet, pero no se ha distribuido al personal.	50%
8.1.4 Devolución de activos	Se incluye dentro del procedimiento de baja o finalización de contrato que tiene el departamento de TI. Cuando la actividad de una persona cesa se informa a RRHH y al departamento de TI a la vez, éste último será el que le recoja todos sus activos prestados para realizar las labores en la organización.	50%
8.2 Clasificación de la información		
8.2.1 Clasificación de la información	Existe una clasificación de la información definida, incluida y publicada en el procedimiento de uso de activos.	100%
8.2.2 Etiquetado de la información	La información se etiqueta a través de metadatos según su clasificación.	100%

8.2.3 Manipulado de la información	Recientemente incluido en el procedimiento de uso de activos, de acuerdo con el esquema de clasificación adoptado por la organización.	100%
8.3 Manipulación de los soportes		
8.3.1 Gestión de soportes extraíbles	Existía un documento relativo a ello, ahora se ha incluido en el procedimiento de uso de activos de manera más detallada, falta difundirlo al personal.	80%
8.3.2 Eliminación de soportes	Se quiere documentar formalmente en el procedimiento de uso de activos, pero no se ha llevado a la práctica aún. Hasta el momento tienen un nivel débil de destrucción de soporte ya que solo hacen un borrado lógico a través de un formateo y el borrado de la partición. No hay diferenciación a la hora de deshacerse de los equipos obsoletos que contienen distinto nivel de sensibilidad de la información.	25%
8.3.3 Soportes físicos en tránsito	N/A. No se comunica información fuera del recinto en soportes físicos.	0%
9. CONTROL DE ACCESO		**66%**
9.1 Requisitos de negocio para el control de acceso		
9.1.1 Política de control de acceso	Está definida una política de control de acceso, pero falta comunicarla a todos los empleados y publicarla en la intranet	50%
9.1.2 Acceso a las redes y a los servicios de red	Existe procedimiento implementado por departamento de Sistemas y TI.	80%
9.2 Gestión de acceso de usuario		
9.2.1 Registro y baja de usuarios	Existe procedimiento implementado por departamento de Sistemas y TI para el registro y baja de usuarios.	90%

9.2.2 Provisión de acceso de usuario	Se asignan permisos según el tipo de usuario o rol, pero después no se hacen revisiones de permisos de accesos.	70%
9.2.3 Gestión de privilegios de acceso	Disponen de un inventario de accesos con las autorizaciones pertinentes mantenido por el departamento de TI y procesos.	90%
9.2.4 Gestión de la información secreta de autenticación de los usuarios	Los empleados conocen sus obligaciones con respecto a la contraseña, las cuales se les envía por correo junto a la contraseña que se les proporciona para autenticarse, que además debe ser cambiada la primera vez.	90%
9.2.5 Revisión de los derechos de acceso de usuario	Procedimiento de revisión periódica de accesos pendiente de implementar.	0%
9.2.6 Retirada o reasignación de los derechos de acceso	Procedimiento de revisión periódica de accesos pendiente de implementar.	0%
9.3 Responsabilidades del usuario		
9.3.1 Uso de la información secreta de autenticación	Se describe en el procedimiento para el control de accesos implementado por departamento de Sistemas y TI.	80%
9.4 Control de acceso a sistemas y aplicaciones		
9.4.1 Restricción del acceso a la información	Cada empleado tiene un perfilado de acceso distinto según el rol que tenga dentro de la organización y la información a la que vaya a acceder.	80%
9.4.2 Procedimientos seguros de inicio de sesión	Tienen procedimientos para los administradores de algunos sistemas como el de gestión de pólizas, pero no para todos los sistemas.	60%
9.4.3 Sistemas de gestión de contraseñas	Existen implementados en el sistema unos requisitos para las contraseñas de administradores, por ejemplo que se deban cambiar cada 60 días y que tengan una	80%

	longitud mínima de 8 caracteres.	
9.4.4 Uso de utilidades con privilegios del sistema	Herramientas implementadas y en uso solo por el departamento de TI.	80%
9.4.5 Control de acceso al código fuente de los programas	Inventario de accesos mantenido por el departamento de TI que son los únicos que pueden acceder al código de las aplicaciones.	80%
10. CRIPTOGRAFÍA		**65%**
10.1 Controles criptográficos		
10.1.1 Política de uso de los controles criptográficos	No existe una política de los controles criptográficos que se usan en la organización, aunque hay algunas medidas informalmente implementadas sobre la gestión de las claves que se usan.	50%
10.1.2 Gestión de claves	El departamento de TI gestiona las claves del servicio de comercio electrónico de venta de pólizas y de la VPN.	80%
11. SEGURIDAD FÍSICA Y DEL ENTORNO		**71%**
11.1 Áreas seguras		
11.1.1 Perímetro de seguridad física	La organización dispone de control de acceso al recinto mediante tarjeta de acceso para pasar las barras y seguridad privada 24x7. También existe una recepcionista en el Edificio 1.	90%
11.1.2 Controles físicos de entrada	El personal tiene tarjetas identificativas que son con las que acceden al recinto, pero no las llevan visibles. Existe carencia a la hora de controlar el acceso al CPD ya que no se registran los accesos a éste y no existe un doble factor de autenticación para acceder, o	60%

	alarmas que detecten intrusos.	
11.1.3 Seguridad de oficinas, despachos y recursos	La seguridad física está aplicada en los dos edificios. Para acceder, en ambos se debe pasar la tarjeta para ver si se tiene acceso o no.	90%
11.1.4 Protección contra las amenazas externas y ambientales	El CPD, ubicado en la planta baja del Edificio 1 de Sao Paulo, no cuenta con medidas preventivas en cuanto a inundaciones, no existen falso suelo, pero si existen medidas de detección y extinción de incendios.	80%
11.1.5 El trabajo en áreas seguras	Cuando alguien necesita realizar una labor dentro del CPD, tiene que pasar por autorizarle el acceso y va acompañado por el Responsable de Seguridad, pero los accesos no quedan registrados.	50%
11.1.6 Áreas de carga y descarga	Existen zonas acordes para la carga y descarga de material en lugares donde no hay información accesible, pero no se revisa las cargas antes de introducirlas al edificio.	75%
11.2 Seguridad de los equipos		
11.2.1 Emplazamiento y protección de equipos	El CPD está ubicado en área restringida al personal autorizado, pero no cuenta con toda la seguridad de acceso que debería contar como se ha mencionado antes. A los empleados del Edificio 1 se les ha proporcionado filtros para los equipos.	60%
11.2.2 Instalaciones de suministro	El CPD cuenta con varios sistemas de alimentación ininterrumpida para los servicios críticos de la organización.	90%
11.2.3 Seguridad del cableado	El cableado no está visible en las zonas de trabajo. No se consideran medidas especiales de seguridad para el cableado del CPD donde hay sistemas sensibles.	75%
11.2.4 Mantenimiento de los	Todos los equipos críticos que hay en el CPD tienen su contrato de mantenimiento.	80%

equipos		
11.2.5 Retirada de materiales propiedad de la empresa	No hay un registro de salida de material que pueda salir de la empresa, pero los empleados saben que no deben hacerlo sin autorización, aunque esto no siempre se cumple.	50%
11.2.6 Seguridad de los equipos fuera de las instalaciones	Cuando es necesaria la salida de personal con portátiles e información en situaciones puntuales, se les da una guía de seguridad donde vienen incluidas ciertas medidas para el tratamiento de los equipos o documentos fuera de las instalaciones.	90%
11.2.7 Reutilización o eliminación segura de equipos	Poseen un nivel débil de destrucción de soporte ya que solo hacen un borrado lógico a través de un formateo normal y no se ha pensado en cómo gestionar la destrucción física segura de los equipos que están almacenados obsoletos.	40%
11.2.8 Equipo de usuarios desatendido	En el procedimiento de uso de activos se menciona que se debe bloquear con contraseña el ordenador. Si se detecta inactividad en las aplicaciones principales o en el propio equipo, se pide de nuevo la contraseña al usuario en la aplicación o se bloquea la pantalla del ordenador.	70%
11.2.9 Política de puesto de trabajo despejado y pantalla limpia	Existen cajoneras en cada puesto de trabajo para custodiar bajo llave la información que es necesaria tener en papel solo en el Edificio 1, no en el call center.	70%
12. SEGURIDAD DE LAS OPERACIONES		**62%**
12.1 Procedimientos y responsabilidades operacionales		
12.1.1 Documentación de procedimientos de la operación	El departamento de TI tiene procedimientos para gestionar los sistemas de la organización, especialmente para los sistemas críticos (en relación al mantenimiento de equipos, gestión del correo, configuraciones de seguridad), pero se corre el riesgo de que esa información no esté actualizada.	60%

12.1.2 Gestión de cambios	Los cambios de versiones de código, actualizaciones o de arquitecturas son revisados y aprobados formalmente, pero no se verifica previamente si se cumplen o no los requisitos de seguridad.	60%
12.1.3 Gestión de capacidades	Actualmente, no se tiene en cuenta los requerimientos de capacidad futuros o los problemas que puedan surgir respecto a este aspecto en servicios críticos que se prestan internamente ni tampoco lo contemplan con el proveedor de copias de seguridad.	10%
12.1.4 Separación de los recursos de desarrollo, prueba y operación	La organización desarrolla software a nivel interno y dispone de segregación de entornos, teniendo por un lado la red de desarrollo y la red de producción. El personal de desarrollo solo dispone de permisos de administración dentro del entorno de desarrollo, y el código lo mandan por SFTP a producción en una carpeta específica para que los de producción lo publiquen. Antes de su publicación, realizan pruebas previas al software de producción y pruebas de usuario, y ahí se validan definitivamente los datos y se certifica la aplicación.	90%
12.2 Protección contra el software malicioso (malware)		
12.2.1 Controles contra el código malicioso	Para protegerse contra código malicioso, disponen de: • Antivirus en todos sus sistemas, tanto en PCs como en servidores, los cuales si no hay problemas, debieran tener actualización periódica de firmas de antivirus. • Filtrado de contenidos de internet y listas negras. •Herramienta de gestión de inventario que les permite ver las actualizaciones y parches de seguridad instalados en los sistemas. No tienen documentos donde queden reflejados los procedimientos de actuación	75%

	frente a incidentes y de recuperación ante ataques.	
12.3 Copias de Seguridad		
12.3.1 Copias de seguridad de la información	Se realizan copias de información diaria cada 15 minutos al CPD del proveedor solamente de la información que contiene algunas bases de datos de interés primordial para el negocio (con la información relativa a clientes, pólizas contratadas, procedimientos), pero no disponen de copias de de seguridad de toda la información generada en el call center, ni los equipos personales, ni los dispositivos portátiles, buzones de correo, etc. No se dispone de una política de respaldo formalmente documentada, solo existe un contrato firmado con el proveedor para las copias de seguridad concretas que se han dicho anteriormente.	50%
12.4 Registros y supervisión		
12.4.1 Registro de eventos	La organización dispone de herramientas que recogen eventos y alertas como los sistemas de detección o prevención de intrusiones (IDS/IPS) que se producen en los sistemas o en la red, pero no tienen herramientas como un SIEM (*Security Information and Event Management*) para analizar esos eventos y correlacionarlos. No están documentados ni formalizados los procedimientos/responsabilidades asociados a incidentes de seguridad, y no se tiene un registro histórico de ellos. Hay registros para auditorías en los sistemas más críticos pero no están del todo bien configurados, y hay sistemas donde ni si quieran están activados.	60%
12.4.2 Protección de la información de registro	Solo los administradores autorizados pueden acceder.	100%

12.4.3 Registros de administración y operación	Se registran la acciones de administración	100%
12.4.4 Sincronización del reloj	Los sistemas no están configurados para tomar una determinada referencia de tiempo para ir sincronizados.	10%
12.5 Control del software en explotación		
12.5.1 Instalación del software en explotación	La instalación de las aplicaciones de negocio o la subida de código a producción la realiza el departamento de TI solo si tiene autorización para ello.	60%
12.6 Gestión de la vulnerabilidad técnica		
12.6.1 Gestión de las vulnerabilidades técnicas	No tienen plan de revisión de vulnerabilidades que contemple test de intrusión en aplicaciones e infraestructura crítica, pero sí se gestionan y supervisan por parte del departamento de TI las vulnerabilidades técnicas relativas a parcheado de los sistemas que les notifica la herramienta de gestión de inventario.	50%
12.6.2 Restricción en la instalación de software	No se permite instalar software al usuario. Si se necesita una aplicación, debe ser autorizado por el Responsable de Seguridad y el departamento de TI instalará la aplicación.	80%
12.7 Consideraciones sobre la auditoría de sistemas de información		
12.7.1 Controles de auditoría de sistemas de información	No se hacen auditorías, pero si hay controles implantados que pueden servir para auditar los sistemas.	60%
13. SEGURIDAD DE LAS COMUNICACIONES		**77%**
13.1 Gestión de la seguridad de redes		

13.1.1 Controles de red	Tienen implantados varios controles de red como se puede visualizar en el diagrama, pero la configuración de los elementos de red se debe revisar porque pueden que no estén operando bien (por ejemplo, se deben revisar las reglas *any* existentes del cortafuegos).	60%
13.1.2 Seguridad de los servicios de red	La seguridad se intenta establecer en los servicios de red, pero no existen guías de configuración de los elementos de seguridad formales con una configuración revisada y aprobada por la Dirección.	50%
13.1.3 Segregación en redes	Se aplica segregación de redes (ver diagrama de red), y segregación en el directorio activo en unidades organizativas (finanzas, recursos humanos, IT, operarios call center...).	90%
13.2 Intercambio de información		
13.2.1 Políticas y procedimientos de intercambio de información	Están establecidos procedimientos con el banco, clientes y proveedores.	90%
13.2.2 Acuerdos de intercambio de información	Existen contratos que lo exponen con el banco, clientes y proveedores.	90%
13.2.3 Mensajería electrónica	Existe un procedimiento de uso de mensajería electrónica en la organización, pero no consta que lo conozca todo el personal y se esté cumpliendo.	80%
13.2.4 Acuerdos de confidencialidad o no revelación	Se firman acuerdos de confidencialidad con empleados y proveedores externos.	80%
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS S. DE INFORMACIÓN		**51%**
14.1 Requisitos de seguridad en sistemas de información		

14.1.1 Análisis de requisitos y especificaciones de seguridad de la información	La organización no comunica a la sede central corporativa cada nueva iniciativa que surge para que desde el área de seguridad dedicada a nuevas iniciativas de negocio se incluyan desde el diseño los requisitos de seguridad de la información pertinentes.	10%
14.1.2 Asegurar los servicios de aplicaciones en redes públicas	Se usan comunicaciones cifradas y protocolos seguros (HTTPS, SSL/TLS) cuando se utiliza el portal web del servicio de pólizas y el correo electrónico.	80%
14.1.3 Protección de las transacciones de servicios de aplicaciones	Se usan comunicaciones cifradas y protocolos seguros (HTTPS, SSL/TLS) cuando se utiliza el portal web del servicio de pólizas y el correo electrónico.	80%
14.2 Seguridad en el desarrollo y en los procesos de soporte		
14.2.1 Política de desarrollo seguro	Existe un procedimiento de desarrollo seguro que se ha pasado desde la sede central corporativa y se quiere adoptar, pero no está implantado formalmente en la organización.	40%
14.2.2 Procedimiento de control de cambios en sistemas	No existen procedimientos formales de control de cambios documentados.	10%
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Se verifica que todo funcione bien después de un cambio pero no se hace evaluaciones de riesgo o análisis de impactos porque no hay un procedimiento formalmente definido.	80%
14.2.4 Restricciones a los cambios en los paquetes de software	Solo los administradores autorizados pueden realizar cambios.	20%
14.2.5 Principios de ingeniería de sistemas seguros	No están establecidos específicamente unos principios de ingeniería segura pero se quieren adoptar unos principios mínimos que se cumplan siguiendo los procedimientos establecidos o que aún están por establecer del Cuerpo Normativo de Seguridad.	20%

14.2.6 Entorno de desarrollo seguro	Existe un entorno de desarrollo seguro, separado del entorno de pruebas y de producción.	90%
14.2.7 Externalización del desarrollo de software	Se establecen acuerdos de seguridad en el desarrollo y acuerdos de licencias	70%
14.2.8 Pruebas funcionales de seguridad de sistemas	Se hacen pruebas y verificaciones para comprobar que el sistema funciona como se espera.	80%
14.2.9 Pruebas de aceptación de sistemas	Se hacen pruebas y verificaciones para comprobar que el sistema funciona como se espera.	80%
14.3 Datos de prueba		
14.3.1 Protección de los datos de prueba	Los datos que utilizan en el entorno de pruebas son datos reales, no enmascarados.	0%
15. RELACIÓN CON PROVEEDORES		**56%**
15.1 Seguridad en las relaciones con proveedores		
15.1.1 Política de seguridad de la información en las relaciones con los proveedores	Existe un procedimiento donde se disponen los requerimientos de seguridad de la información en la relación con los proveedores.	80%
15.1.2 Requisitos de seguridad en contratos con terceros	Se firman acuerdos de confidencialidad proveedores externos.	80%
15.1.3 Cadena de suministros de tecnología de la información y de las comunicaciones	Se pasan cuestionarios a los proveedores para ver en qué medida cumplen con ciertos requisitos de seguridad que quiere evaluar la organización.	70%
15.2 Gestión de la provisión de servicios del proveedor		
15.2.1 Control y revisión de la provisión de servicios del	No se realizan auditorías a proveedores de servicios.	0%

	proveedor	
	15.2.2 Gestión de cambios en la provisión del servicio del proveedor	Se revisan los acuerdos sólo cuando hay un cambio de servicio.	50%
16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN		**61%**
16.1 Gestión de incidentes de seguridad de la información y mejoras		
	16.1.1 Responsabilidades y procedimientos	Es responsabilidad del departamento de TI gestionar y supervisar los eventos que se producen en los sistemas y las alertas que se generan en el IDS y en la red en general, pero faltan procedimientos y flujos de comunicación con el Responsable de Seguridad de la Información.	40%
	16.1.2 Notificación de los eventos de seguridad de la información	La notificación de los eventos de seguridad se hace al departamento de TI que es quien gestiona los eventos.	60%
	16.1.3 Notificación de puntos débiles de la seguridad	La notificación de los eventos de seguridad se hace al departamento de TI que es quien gestiona los eventos.	60%
	16.1.4 Evaluación y decisión sobre los eventos de seguridad de información	El departamento de TI es quien evalúa hasta el momento los eventos de seguridad de la información. Solo se registran algunos eventos de seguridad que han sido graves.	70%
	16.1.5 Respuesta a incidentes de seguridad de la información	Los incidentes de seguridad se comunican al departamento de TI que es quien da respuesta a los mismos. Solo se registran las decisiones de los incidentes de mayor gravedad, siguiendo un procedimiento no formal.	60%
	16.1.6 Aprendizaje de los incidentes de seguridad de la información	Si no es un incidente grave o muy recurrente, no se analiza en detalle.	60%

16.1.7 Recopilación de evidencias	Existe un procedimiento interno en el departamento de TI sobre la recopilación de evidencias, pero quieren revisarlo y actualizarlo ya que son conscientes de que se puede producir un evento de seguridad de la información que puede que tenga como consecuencia una acción legal y quieren estar preparados.	70%
17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO		**23%**
17.1 Continuidad de la seguridad de la información		
17.1.1 Planificación de la continuidad de la seguridad de la información	No cuentan con un plan de continuidad de negocio ni de recuperación ante desastres.	10%
17.1.2 Implementar la continuidad de la seguridad de la información	No cuentan con un plan de continuidad de negocio ni de recuperación ante desastres.	10%
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Se ha establecido solo algunos controles de seguridad para los sistemas que proveen servicio a las aplicaciones de call center y la de venta de pólizas a través del portal.	30%
17.2 Redundancias		
17.2.1 Disponibilidad de los recursos de tratamiento de la información	Se monitorizan la mayoría de los sistemas para detectar percances en la disponibilidad de los mismos, pero no se han establecido procedimientos en caso de indisponibilidad de los mismos.	40%
18. CUMPLIMIENTO		**30%**
18.1 Cumplimiento de los requisitos legales y contractuales		

	18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales	En Brasil no hay legislación obligada en materia de protección de datos personales. El pasado mes de Julio el Senado de Brasil aprobó el proyecto de Ley de Protección de Datos, y la organización tiene que adaptarse a ella. Brasil solo tiene algunas leyes sectoriales como el Marco Civil para Internet, pero no garantiza la protección de la privacidad.	50%
	18.1.2 Derechos de propiedad intelectual (DPI)	No existen procedimientos. Se revisan las licencias.	50%
	18.1.3 Protección de los registros de la organización	Se protegen los registros contables, de log de bases de datos, etc.	80%
	18.1.4 Protección y privacidad de la información de carácter personal	La organización protege la información de carácter personal por iniciativa propia, pero hasta el momento no ha habido legislación nacional aplicable.	60%
	18.1.5 Regulación de los controles criptográficos	No se tienen en cuenta regulaciones sobre controles criptográficos.	0%
18.2 Revisiones de la seguridad de la información			
	18.2.1 Revisión independiente de la seguridad de la información	No se realizan auditorías de ningún tipo para realizar revisiones independientes de la seguridad de la información.	0%
	18.2.2 Cumplimiento de las políticas y normas de seguridad	No se realizan revisiones de cumplimiento.	0%
	18.2.3 Comprobación del cumplimiento técnico	No se realizan test de intrusión para valorar si los sistemas cumplen con la normativa de seguridad que establece la organización.	0%

2.4 RESULTADOS DEL ANÁLISIS DIFERENCIAL

En este apartado se muestra los resultados del análisis diferencial realizado sobre la situación actual de la organización con respecto a las normas ISO 27001 e ISO 27002.

Con respecto a la norma ISO 27001, se observa que existe un nivel de cumplimiento total del 20,45 %, debido principalmente a que se va a implantar por primera vez un SGSI.

Con respecto a la norma ISO 27002, se observa que existe un nivel de cumplimiento total del 55%. Se ha desglosado en un diagrama radar para analizarlo mejor, donde el radio exterior de la circunferencia representa el cumplimiento completo del nivel de seguridad de la norma y lo que está en rojo es la situación en la que se encuentra la organización actualmente. De esta forma, se pueden ver los dominios con menor cumplimiento, que son la organización de la seguridad de la información, la adquisición, desarrollo y mantenimiento de los sistemas de información, la continuidad de negocio y el cumplimiento normativo, por debajo del 50% de cumplimiento.

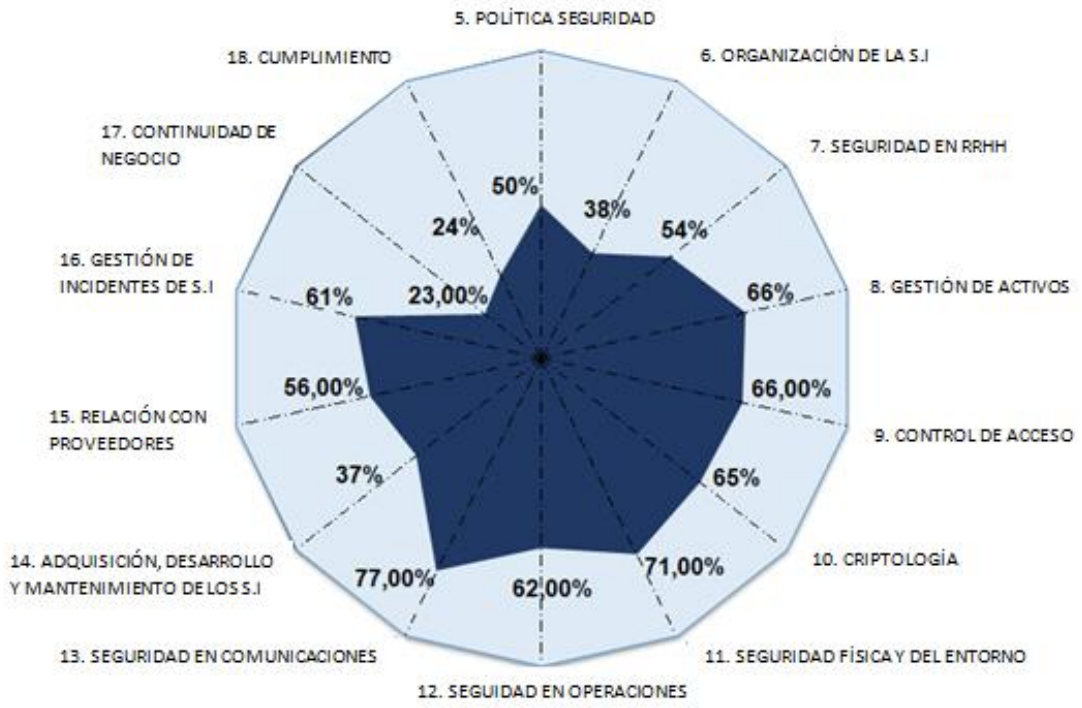

Fig. 5: Grado de adecuación actual de la organización a la norma de referencia ISO 27002

En general, se puede apreciar que la organización no alcanza un nivel aceptable para la organización (por encima de un 75%) de implantación de los controles de seguridad reflejados en la norma ISO 27002 a la hora de comenzar con la implantación del Sistema de Gestión de Seguridad de la Información.

3. SISTEMA DE GESTIÓN DOCUMENTAL

Para la implantación de un correcto Sistema de Gestión de Seguridad de la Información, la norma ISO 27001 establece una serie de documentos que son obligatorios para el cumplimiento normativo de la misma y de los que la organización debería disponer.

A continuación, se lista el sistema de gestión documental y las descripciones de cada información documentada a la que se hace referencia en la norma:

- **Alcance del SGSI:** Define el ámbito de la organización que queda sometido al SGSI delimitando los límites de los sistemas de información, áreas de la empresa, procesos involucrados dentro del SGSI, etc.
- **Política de seguridad de la información y objetivos:** Definición de una política de la organización para la seguridad de la información, además de la definición de cuáles son los objetivos que se pretenden obtener con la implementación del SGSI.
- **Metodología de evaluación y tratamiento de riesgos:** Definición de las reglas y las etapas que se tienen que seguir para gestionar, analizar y tratar los riesgos identificados.
- **Declaración de aplicabilidad:** Se establece la aplicabilidad de cada uno de los controles de seguridad al SGSI de la organización. Esta declaración está basada en el rendimiento de los medios de valoración y tratamiento de los riesgos, responsabilidades contractuales y requisitos legales o del negocio de la empresa para la seguridad de la información.
- **Plan de tratamiento de riesgo:** Se establece un plan (Plan de Implementación o Plan de Acción) para la ejecución de las medidas de seguridad necesarias para el tratamiento de los riesgos identificados.
- **Definición de roles y responsabilidades de seguridad:** Se definen y asignan los roles y las responsabilidades de las personas implicadas en el mantenimiento del SGSI
- **Inventario de activos:** documento de todos los activos implicados en el alcance del SGSI, el cual debe mantenerse y actualizarse.
- **Política de uso aceptable de activos:** documento con las normas internas que tienen que seguir los empleados para un uso aceptable de los activos y de la información de la organización.
- **Política de control de acceso:** documento que establece los requerimientos sobre el acceso a los recursos, sistemas de información, etc. basado en los requisitos de negocio y de seguridad de la información (contraseñas, privilegios, …)
- **Procedimiento de operación para gestión de TI:** Documentos que detallen las actividades el sistema asociadas a los recursos de tratamiento y comunicación de la información, tales como procedimientos de encendido y apagado de ordenadores, copias de seguridad, antivirus, etc.

- **Principios de ingeniería de sistemas seguros:** Principios básicos de ingeniería de sistemas seguros para operar de forma segura con los sistemas de información de la organización.
- **Política de seguridad de proveedores:** documento para la gestión de proveedores cuando éstos necesitan acceder a activos de la organización.
- **Procedimiento de gestión de incidentes de seguridad de la información:** documento que establece los pasos que son necesarios para la identificación, notificación, y tratamiento, de incidentes de seguridad de la información, para así garantizar una respuesta rápida y eficaz ante un incidente.
- **Procedimiento continuidad del negocio:** documento que establece los pasos a seguir para el caso de que se produzca una indisponibilidad o interrupción del negocio.
- **Requerimientos legales, regulatorios y contractuales:** Se establece un proceso para la identificación de los requerimientos legales, regulatorios o contractuales que aplican a la organización en relación a la seguridad de la información para cumplirlos.

También se pueden considerar información documentada obligatoria la documentación sobre los **siguientes registros**:

- Registros de formación, habilidades, experiencia y calificaciones.
- Seguimiento y resultados de medición.
- Programa de auditoría interna.
- Resultados de auditorías internas.
- Resultados de la Revisión por Dirección.
- Resultados de acciones correctivas.
- Registros de las actividades de usuario, excepciones y eventos de seguridad.

Dicho esto, la organización bajo estudio, cuenta con los siguientes documentos que establece como necesarios la ISO/IEC 27001 para poder certificar el Sistema de Gestión de Seguridad de la Información, y que se desglosan a continuación:

3.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la Información es determinada por la dirección de la empresa, la cual apoya los objetivos y principios de la seguridad de la información que en ella se dictan. En la Política de Seguridad se establecen [5]:

- Los objetivos que se pretenden obtener con la implantación de un Sistema de Gestión de Seguridad de la Información de acuerdo a las necesidades y estrategia de la organización y la legislación vigente.
- Las pautas de cómo se debe actuar en caso de que se produzca algún incidente.
- Los roles y responsabilidades frente a la protección de la información.

Para que la Política de Seguridad cumpla con la ISO/IEC 27001, debe cumplir los siguientes requisitos:

- Debe de ser corta, precisa y de fácil comprensión, redactada de una manera accesible para todo el personal de la organización.
- Debe ser aprobada por la dirección y publicitada por la misma.
- Debe estar disponible para su consulta siempre que sea necesario.
- Debe ser la referencia para la resolución de conflictos y cuestiones relativas a la seguridad de la organización.
- Debe definir responsabilidades teniendo en cuenta que éstas van asociadas a la autoridad dentro de la compañía. En función de las responsabilidades se decidirá quién está autorizado a acceder a qué tipo de información.
- Debe indicar que lo que se protege en la organización incluye tanto al personal como a la información, así como su reputación y continuidad.
- Debe ser personalizada para cada organización.
- Por último, debe señalar las normas y reglas que va a adoptar la organización y las medidas de seguridad que serán necesarias.

Por último, cabe mencionar que esta política debe mantenerse actualizada. Se adjunta en el anexo dicha Política de Seguridad de la Información.

3.2 PROCEDIMIENTO DE AUDITORÍAS INTERNAS

La función de auditoría interna debería estar formalmente definida para realizar un seguimiento continuado del Sistema de Gestión de la Seguridad de la Información implantado, permitiendo evaluar la validez y aplicación de los procedimientos, políticas y controles establecidos. Debería realizarse una vez al año, permitiendo encontrar deficiencias y contribuyendo a una mejora continua del SGSI con respecto al nivel inicial del que se partía.

Las auditorías internas deben ser programadas y estar establecidas bajo un Procedimiento o Plan de Auditorías Internas, el cual se encuentra anexo a este trabajo

bajo el nombre **"SI-PRO-Procedimiento de Auditorías Internas-v.01.pdf",** y debe ser aprobado por la Dirección.

3.3 GESTIÓN DE INDICADORES

Es necesario definir indicadores para medir la eficacia de los controles de seguridad implantados, de esta manera se comprueba si el SGSI funciona correctamente y se puede seguir mejorando.

Se tomará una serie de indicadores que nos den una visión global del estado de seguridad del sistema de la organización, y se fijarán unos umbrales de alerta para cada indicador. Para que la medición e indicadores sean lo más completos posible, se ha decidido realizar una medición a diferentes alturas, empezando por el nivel estratégico, pasando por el nivel táctico y acabando por el nivel operacional de la organización [6].

Dicho procedimiento se encuentra anexo a este documento bajo el título **"SI-PRO-Gestión de los Indicadores-v.01".**

La acción de medir el SGSI implantado permitirá a la organización valorar la eficiencia y eficacia del sistema de seguridad desplegado, tomar decisiones técnicas y de adjudicación de recursos, y facilitar la rendición de cuentas de los responsables.

3.4 PROCEDIMIENTO DE REVISIÓN POR LA DIRECCIÓN

La norma ISO 27001, dentro de la fase *Chequear* (monitorear y revisar el SGSI) del ciclo PDCA, establece como necesario la realización de revisiones al menos una vez al año del SGSI por parte de la Dirección. El procedimiento para llevar a cabo la realización de las revisiones se describe en el adjunto con título "**SI-PRO-Procedimiento de Revisión por la Dirección-v.01"**.

3.5 GESTIÓN DE ROLES Y RESPONSABILIDADES

Para que el SGSI de la organización cumpla con los requisitos de la norma ISO 27001, la Dirección debe establecer los roles y responsabilidades para la seguridad de la información dentro de la organización. Con ello se consigue tener identificados claramente las personas y sus tareas correspondientes dentro del SGSI.

Se adjunta a este trabajo el procedimiento para la gestión de roles y responsabilidades bajo el título **"SI-PRO-Gestión de Roles y Responsabilidades-v.01".**

3.6 METODOLOGÍA DE ANÁLISIS DE RIESGOS

Se utilizará como metodología de análisis y gestión de riesgos MAGERIT, cuyas siglas significan Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administración. Fue elaborada por el Consejo Superior de Administración

Electrónica, como respuesta a la percepción de que la Administración, y, en general, todas las organizaciones, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión. [7]

Consiste en investigar los riesgos que soportan los Sistemas de Información para después asignar las medidas apropiadas que deberían adoptarse para controlar esos riesgos.

El análisis de riesgos forma parte de la etapa de *Planificación* dentro del Ciclo PDCA, donde se toman decisiones de tratamiento que luego se materializarán en la etapa de *Implantación.*

Las tareas para llevar a cabo MAGERIT son las siguientes [8]:

1. **Caracterización de los activos:** identificación de los activos relevantes dentro del sistema a analizar, caracterizándolos por el tipo de activo, identificando las relaciones entre los diferentes activos, determinando en qué dimensiones de seguridad son importantes y valorando esta importancia. Esta actividad da como resultado el informe "Modelo de Valor". Las sub-tareas que incluye esta actividad son:

   I. Tarea MAR[2].11: Identificación de los activos
   II. Tarea MAR.12: Dependencias de los activos
   III. Tarea MAR.13: Valoración de los activos

   En cuanto a la valoración de los activos, se hará en base a los siguientes niveles de medición, pero a la hora de calcular el riesgo se escogerá el máximo valor del rango:

Valoración de los activos		
Valor	**Niveles**	**Rango en €**
MA	Muy Alto	350.000 - 100.000
A	Alto	100.000 - 50.000
M	Medio	50.000 - 10.000
B	Bajo	10.000 - 1.000
MB	Muy Bajo	1.000 - 0

Tabla 1. Valoración de los activos

   A continuación, se valora el impacto que tendría que una amenaza se materializase en cada una de las dimensiones de seguridad de la información de un activo, siendo éstas las siguientes:

   - **Confidencialidad [C]:** asegura que únicamente los usuarios que tienen acceso autorizado puedan acceder a la información.

[2] MAR: Método de Análisis de Riesgos

- **Integridad [I]:** asegura la exactitud de los datos y métodos de procesamiento de la información que los usuarios autorizados gestionan.
- **Disponibilidad [D]:** asegura que los recursos se puedan utilizar o tenerlos cuando sean requeridos en cualquier momento.
- **Autenticidad [A]:** asegura la identidad de quién hace o ha hecho una acción frente a la suplantación de identidad.
- **Trazabilidad [T]:** asegura disponer de trazabilidad para analizar, entender, perseguir y aprender quién hace qué y cuándo.

La escala de valoración con la que se mide el impacto de las amenazas en cada una de las dimensiones de seguridad es la siguiente:

Escala de criterios		
Valor		**Criterio/Daño**
10	Extremo	Daño extremadamente grave
9	Muy Alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Tabla 2. Escala de criterios

2. **Caracterización de las amenazas:** identificación de las amenazas relevantes sobre el sistema a analizar, caracterizándolas por las estimaciones de ocurrencia (probabilidad) y daño causado (degradación). Esta actividad da como resultado el informe "Mapa de Riesgos". Las sub-tareas que incluye esta actividad son:

   I. Tarea MAR.21: Identificación de las amenazas.
   II. Tarea MAR.22: Valoración de las amenazas.

   Una vez identificadas las amenazas, se procede a valorarlas sobre los activos, estimando la probabilidad que tendrían de materializarse teniendo en cuenta las salvaguardas ya implantadas en la organización, y la degradación que produciría en cada dimensión de seguridad del activo si se materializasen, que va desde 0 % de pérdida del activo, equivalente a un daño despreciable, hasta 100% equivalente a un daño extremadamente grave.

   La escala de valores escogida para valorar la probabilidad de materialización de la amenaza en un activo es la siguiente:

Probabilidad		Valor
MA	Muy frecuente (a diario)	1
A	Frecuente (mensualmente)	0,03287671
M	Normal (semestralmente)	0,00547945
B	Poco frecuente (anualmente)	0,00273973
MB	Muy poco frecuente (más de 10 años)	0

Tabla 3. Probabilidad de ocurrencia

3. **Caracterización de las salvaguardas:** identificación de las salvaguardas desplegadas en el sistema a analizar, calificándolas por su eficacia frente a las amenazas que pretenden mitigar. El resultado de esta actividad se concreta en los siguientes informes:

   - Declaración de aplicabilidad.
   - Evaluación de salvaguardas.
   - Insuficiencias (o vulnerabilidades del sistema de protección).

   Incluye las siguientes sub-tareas:

   I. Tarea MAR.31: Identificación de las salvaguardas pertinentes.
   II. Tarea MAR.32: Valoración de las salvaguardas

   Para medir la eficacia y madurez de las salvaguardas implantadas, se empleará la siguiente escala [7]:

Efectividad	Nivel	Significado
0%	L0	Inexistente
10%	L1	Inicial/ad hoc
50%	L2	Reproducible, pero intuitivo
90%	L3	Proceso definido
95%	L4	Gestionado y medible
100%	L5	Optimizado

Tabla 4. Eficacia y madurez de las salvaguardas

4. **Estimación del estado de riesgo:** procesamiento de todos los datos recopilados en las actividades anteriores para:

   - Realizar un informe del estado de impacto y riesgo.
   - Realizar un informe de insuficiencias en el sistema de salvaguardas.

Incluye las siguientes sub-tareas:

I. Tarea MAR.41: Estimación del impacto
II. Tarea MAR.42: Estimación del riesgo

3.7 DECLARACIÓN DE APLICABILIDAD (*SoA*)

La declaración de aplicabilidad permite tener un registro de los controles de seguridad implantados en la organización.

CONTROLES	APLICABILIDAD	COMENTARIOS JUSTIFICATIVOS DE POR QUÉ APLICA
5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN		
5.1.1 Políticas para la seguridad de la información	Aplica	Disponen de una Política de Seguridad, "SI-PO-Política de Seguridad de la Información-v.01", la cual se encuentra aprobada por la Dirección y se encuentra publicada en la intranet local accesible por todos los empleados.
5.1.2 Revisión de las políticas para la seguridad de la información	Aplica	La Política de Seguridad debe ser revisada y mantenerse actualizada por la Dirección. Aún no existe un registro donde aparezcan las actualizaciones acometidas sobre la misma.
6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		
6.1.1 Roles y responsabilidades en seguridad de la información	Aplica	El Comité de Seguridad está constituido con los roles y responsabilidades asignadas, pero pendiente de formalizar por parte de la Dirección y nunca se ha celebrado uno. La dirección tiene que comprometerse con la implementación del SGSI y velar por el cumplimiento de las políticas y normativas de seguridad.
6.1.2 Segregación de tareas	Aplica	Las tareas están definidas, pero no están claramente asignadas al personal involucrado en el SGSI según las responsabilidades que se les han asignado. Tampoco se realiza ningún tipo de seguimiento o mantenimiento periódico de las tareas y responsabilidades asociadas.
6.1.3 Contacto con las autoridades	Aplica	Existe contacto con las autoridades por parte de la organización, pero la Dirección debe revisar las cláusulas que tienen desarrolladas en la actualidad para ver si cumplen con lo establecido.
6.1.4 Contacto con grupos de interés especial	Aplica	Se mantiene contacto con algunos grupos de interés especial (grupos legales de protección de datos de carácter personal por ejemplo), pero se tiene que tener contacto con otros grupos para

		estar actualizado en otras materias relativas a seguridad de la información.
6.1.5 Seguridad de la información en la gestión de proyectos	Aplica	No existe documentación oficial relativa a establecer unos requisitos de seguridad en las nuevas iniciativas y proyectos que surgen en la organización, solo recomendaciones informales, por correo y a veces no aprobadas ni con seguimiento alguno. Por tanto se hace necesario que se establezca documentación con requisitos de seguridad cada vez que surge una nueva iniciativa o proyecto para involucrar a la seguridad desde el diseño de la misma.
6.2.1 Política de dispositivos móviles	Aplica	No hay una política o recomendaciones para el uso de dispositivos móviles y en la organización usan portátiles, por tanto se debe de desarrollar.
6.2.2 Teletrabajo	No Aplica	La organización no usa esta modalidad de trabajo.
7. SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS		
7.1.1 Investigación de antecedentes	Aplica	RRHH suele revisar la veracidad de los datos y referencias aportadas teniendo en cuenta la ley aplicable. Se debe establecer un proceso de revisión tanto de la información aportada por el empleado como lo que puede estar expuesto en Internet.
7.1.2 Términos y condiciones del empleo	Aplica	En la documentación generada para contratar a personal, se debe incluir requerimientos de seguridad y se deben dar a conocer las políticas de seguridad de la empresa que les son de aplicación, a parte de las ya incluidas cláusulas de confidencialidad.
7.2.1 Responsabilidades de gestión	Aplica	Todos los empleados conocen la política de seguridad de la información, pero algunos departamentos desconocen exactamente cuáles son las responsabilidades que les son asignadas y los procedimientos que se deben llevar a cabo.
7.2.2 Concienciación, educación y capacitación en seguridad de la información	Aplica	Lo único que tienen al respecto son emails que IT manda de vez en cuando con consejos sobre seguridad. Se debe establecer formalmente un plan de concienciación y formación continua en seguridad (e-learning, charlas presenciales) para todo el personal, incluidos los responsables del SGSI.
7.2.3 Proceso disciplinario	Aplica	No está definido un proceso disciplinario en las políticas aunque existen algunas pautas fijadas por la Dirección, y no se hace referencia en el momento de la contratación, además de no ser

		conocido por los trabajadores.
7.3.1 Responsabilidades ante la finalización o cambio	Aplica	Está definido un proceso de finalización de la relación con la organización o de cambio de puesto de trabajo, pero en este último caso, es posible que se sumen permisos al hacer cambios de situación del empleado dentro de la empresa. Se debe establecer un proceso adecuado e informado.
8. GESTIÓN DE ACTIVOS		
8.1.1 Inventario de activos	Aplica	Hay un inventario de activos gestionados por una herramienta de gestión de inventario que da información detallada de cada sistema y/o equipo. Dicha herramienta está instalada en los sistemas/equipos y da información detallada y actualizada del estado del mismo. Se debe revisar que todos los activos que entran dentro del alcance del SGSI estén inventariados.
8.1.2 Propiedad de los activos	Aplica	Los activos que manejan información en la organización tienen asignados un propietario. Se debe revisar que los propietarios de los activos.
8.1.3 Uso aceptable de los activos	Aplica	Existe un procedimiento de uso aceptable de los activos, “SI-CN-PRO-Procedimiento de Uso Aceptable de los Activos-v.01”, publicado recientemente en la intranet. Se debería de comunicar por correo electrónico esta política para que llegue a todos los empleados y firmarla.
8.1.4 Devolución de activos	Aplica	Se hace dentro del procedimiento de baja o finalización de contrato que tiene el departamento de TI cuando alguien cesa la actividad en la organización.
8.2.1 Clasificación de la información	Aplica	Existe una clasificación de la información definida, incluida y publicada en el procedimiento de uso de activos, “SI-CN-PRO-Procedimiento de Uso Aceptable de los Activos-v.01”, pero no se aplica en todo la información que maneja la organización.
8.2.2 Etiquetado de la información	Aplica	Recientemente incluido en el procedimiento de uso de activos, “SI-CN-PRO-Procedimiento de Uso Aceptable de los Activos-v.01”. La información no está etiquetada según la clasificación de información definida. Solo se etiqueta alguna información que sale de la organización.
8.2.3 Manipulado de la información	Aplica	Recientemente incluido en el procedimiento de uso de activos, “SI-CN-PRO-Procedimiento de Uso

		Aceptable de los Activos-v.01", de acuerdo con el esquema de clasificación adoptado por la organización.
8.3.1 Gestión de soportes extraíbles	Aplica	Existía un procedimiento relativo a ello, ahora se ha incluido en el procedimiento de uso de activos aprobado, "SI-CN-PRO-Procedimiento de Uso Aceptable de los Activos-v.01".
8.3.2 Eliminación de soportes	Aplica	Tienen equipos y soportes obsoletos y también información en documentos que deben destruir.
8.3.3 Soportes físicos en tránsito	No Aplica	La organización no transporta fuera de sus límites físicos información.
9. CONTROL DE ACCESO		
9.1.1 Política de control de acceso	Aplica	Está definida una política de control de acceso.
9.1.2 Acceso a las redes y a los servicios de red	Aplica	Está definida una política para el acceso de usuarios a las redes y servicios.
9.2.1 Registro y baja de usuarios	Aplica	Existe un procedimiento formal implementado de registro y retirada de usuarios.
9.2.2 Provisión de acceso de usuario	Aplica	Existe un procedimiento formal para asignar o quitar los derechos de acceso para todos los distintos usuarios de los sistemas y servicios.
9.2.3 Gestión de privilegios de acceso	Aplica	Existe un proceso de autorización y un registro de privilegios asignados por rol de usuario.
9.2.4 Gestión de la información secreta de autenticación de los usuarios	Aplica	Procedimiento elaborado por TI para gestionar la información de autenticación
9.2.5 Revisión de los derechos de acceso de usuario	Aplica	Se debe implantar el procedimiento formal de revisión periódica de accesos.
9.2.6 Retirada o reasignación de los derechos de acceso	Aplica	Existe un procedimiento formal implantado para la revisión periódica de retirada o reasignación de los derechos de acceso
9.3.1 Uso de la información secreta de autenticación	Aplica	Existen unas recomendaciones que se leen cuando se envía la información secreta de autenticación.
9.4.1 Restricción del acceso a la información	Aplica	Existe un procedimiento para el control de accesos a la información, de acuerdo a la política de control de acceso definida.
9.4.2 Procedimientos	Aplica	Procedimiento desarrollado en la política de control de accesos según el rol del personal

seguros de inicio de sesión		(distingue entre administrador y usuario normal)
9.4.3 Sistemas de gestión de contraseñas	Aplica	Control necesario ya que se gestionan contraseñas.
9.4.4 Uso de utilidades con privilegios del sistema	Aplica	Se es necesario para administrar los sistemas de la organización.
9.4.5 Control de acceso al código fuente de los programas	Aplica	En primera instancia, el acceso es necesario para el equipo de TI, que incluye desarrolladores y soporte.
10. CRIPTOGRAFÍA		
10.1.1 Política de uso de los controles criptográficos	Aplica	Se usan controles criptográficos en las conexiones VPN, y en algunos servicios que presta la organización.
10.1.2 Gestión de claves	Aplica	Hay claves de los controles criptográficos que se deben proteger.
11. SEGURIDAD FÍSICA Y DEL ENTORNO		
11.1.1 Perímetro de seguridad física	Aplica	Existen zonas donde es de aplicabilidad perímetros de seguridad con un alcance mayor (como puede ser el recinto donde se hallan los dos edificios) y con alcance más acotado (CPD del Edificio 1).
11.1.2 Controles físicos de entrada	Aplica	Hay diferente personal (empleados, proveedores, clientes, etc.) que entran a las instalaciones.
11.1.3 Seguridad de oficinas, despachos y recursos	Aplica	Hay personal que accede a oficinas, despachos y recursos.
11.1.4 Protección contra las amenazas externas y ambientales	Aplica	Pueden ocurrir amenazas externas y ambientales que afecten a los activos de información de la organización.
11.1.5 El trabajo en áreas seguras	Aplica	Auditorías realizadas por personal externo a la organización, de cumplimiento de normativa de seguridad u otros cumplimientos, acceden al CPD, a los puestos de trabajo del personal, a los archivos, etc.
11.1.6 Áreas de carga y descarga	Aplica	Se debe controlar las zonas de carga y descarga donde proveedores y clientes acceden.
11.2.1 Emplazamiento y protección de equipos	Aplica	Se debe proteger y ubicar los equipos de manera segura para protegerse de los riesgos de las amenazas y los riesgos ambientales.

11.2.2 Instalaciones de suministro	Aplica	Se debe asegurar el funcionamiento de los equipos a pesar de los fallos en las instalaciones de suministro.
11.2.3 Seguridad del cableado	Aplica	Se debe proteger frente a daños el cableado que transmite datos o sirve de soporte a los servicios de información.
11.2.4 Mantenimiento de los equipos	Aplica	Se debe asegurar el correcto mantenimiento de los equipos para asegurar su integridad y disponibilidad.
11.2.5 Retirada de materiales propiedad de la empresa	Aplica	Se debe autorizar toda salida de equipos portátiles y documentos.
11.2.6 Seguridad de los equipos fuera de las instalaciones	Aplica	Se debe proteger los dispositivos, equipos portátiles y documentos que salgan fuera (por ejemplo, ordenadores personales portátiles).
11.2.7 Reutilización o eliminación segura de equipos	Aplica	Se debe eliminar de manera segura los activos que se vayan quedando obsoletos o que se estropeen, y eliminar de manera segura cualquier medio de almacenamiento en caso de que se vaya a reutilizar.
11.2.8 Equipo de usuarios desatendido	Aplica	Los usuarios deben proteger sus ordenadores personales o dispositivos de información cuando estén desatendidos.
11.2.9 Política de puesto de trabajo despejado y pantalla limpia	Aplica	Se debe proteger los activos de información de riesgos de accesos no autorizados o daños a la información tanto cuando se está en el puesto de trabajo como cuando no se está en él.
12. SEGURIDAD DE LAS OPERACIONES		
12.1.1 Documentación de procedimientos de la operación	Aplica	Se deben documentar los procedimientos de operación de los equipos y sistemas de la organización que entren dentro del alcance del SGSI.
12.1.2 Gestión de cambios	Aplica	Se deben controlar las subidas de versiones de código de las aplicaciones de negocio y las actualizaciones de los sistemas operativos.
12.1.3 Gestión de capacidades	Aplica	Se deben ajustar las características de los sistemas, el diseño de red y otros servicios, con vistas a futuras necesidades, para controlar la disponibilidad y eficiencia de los mismos.
12.1.4 Separación de los recursos de desarrollo, prueba y operación	Aplica	Se debe tener separados los entornos de desarrollo, pre-producción y producción de la aplicación que usan en el call center y la aplicación que se mantiene de gestión de pólizas e información de clientes y procesos.

12.2.1 Controles contra el código malicioso	Aplica	Los equipos, tanto fijos como portátiles, y los servidores deben estar protegidos de malware.
12.3.1 Copias de seguridad de la información	Aplica	Se debe hacer backups al menos de la información más importante para la organización.
12.4.1 Registro de eventos	Aplica	Se debe tener un registro de eventos para poder gestionar las alertas que se generen en los sistemas de información, en la red interna y en la DMZ.
12.4.2 Protección de la información de registro	Aplica	Se debe proteger contra accesos no autorizados la información de registro que se almacena en ciertos sistemas de la organización.
12.4.3 Registros de administración y operación	Aplica	Se debe proteger contra accesos no autorizados la información de registro que se almacena en ciertos sistemas de la organización.
12.4.4 Sincronización del reloj	Aplica	Todos los relojes de los sistemas que estén puestos en producción deberían estar sincronizados tomando una única fuente de referencia.
12.5.1 Instalación del software en explotación	Aplica	Se debe contralar que la instalación del software sea hecha únicamente por personal autorizado del área de TI.
12.6.1 Gestión de las vulnerabilidades técnicas	Aplica	Se debe solucionar las vulnerabilidades que se han descubierto en el último test de intrusión realizado a las aplicaciones e infraestructura más importante de la organización.
12.6.2 Restricción en la instalación de software	Aplica	Se debe controlar el software que está instalado en los puestos de trabajo.
12.7.1 Controles de auditoría de sistemas de información	Aplica	Se debe controlar que no ocurra ninguna interrupción en los procesos de negocio cuando se esté auditando algún sistema.
13. SEGURIDAD DE LAS COMUNICACIONES		
13.1.1 Controles de red	Aplica	Se deben proteger las redes y comunicaciones existentes dentro del alcance del SGSI.
13.1.2 Seguridad de los servicios de red	Aplica	Se deben proteger las redes y comunicaciones existentes dentro del alcance del SGSI.
13.1.3 Segregación en redes	Aplica	Actualmente la red se encuentra segregada por eso este control aplica.
13.2.1 Políticas y procedimientos de intercambio de información	Aplica	Hay información en la organización que se debe intercambiar con bancos, clientes y proveedores.

13.2.2 Acuerdos de intercambio de información	Aplica	Hay información en la organización que se debe intercambiar con bancos, clientes y proveedores.
13.2.3 Mensajería electrónica	Aplica	Se debe proteger la información que es intercambiada mediante el servicio de mensajería electrónica.
13.2.4 Acuerdos de confidencialidad o no revelación	Aplica	Se deben tomar medidas para que la información confidencial de la organización no sea revelada.
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS S. DE INFORMACIÓN		
14.1.1 Análisis de requisitos y especificaciones de seguridad de la información	Aplica	Se adquieren o mejoran los sistemas de información que entran dentro del alcance del SGSI.
14.1.2 Asegurar los servicios de aplicaciones en redes públicas	Aplica	Existen servicios de aplicaciones expuestas en Internet a las que acceden los usuarios para visualizarlos y realizar operaciones, y se tiene que garantizar su seguridad.
14.1.3 Protección de las transacciones de servicios de aplicaciones	Aplica	Se llevan a cabo transacciones de servicios de aplicaciones expuestas en Internet.
14.2.1 Política de desarrollo seguro	Aplica	Se llevan a cabo desarrollos dentro de la organización.
14.2.2 Procedimiento de control de cambios en sistemas	Aplica	Se deben controlar los cambios que se hagan a las aplicaciones en producción de la organización.
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Aplica	Se debe revisar y probar toda aplicación que esté en producción después de que haya sufrido cambios el sistema operativo.
14.2.4 Restricciones a los cambios en los paquetes de software	Aplica	Se debe controlar estrictamente los cambios en los paquetes de software.
14.2.5 Principios de ingeniería de sistemas seguros	Aplica	Se debe establecer principios de ingeniería segura en todas las capas de la arquitectura de las nuevas iniciativas que surjan o nuevos sistemas de información.
14.2.6 Entorno de desarrollo seguro	Aplica	Se debe establecer un adecuado entorno de desarrollo seguro para los sistemas que vayan a integrarse en la organización.

14.2.7 Externalización del desarrollo de software	Aplica	La organización a veces hace uso de desarrollo de software externalizado cuando surge alguna nueva iniciativa.
14.2.8 Pruebas funcionales de seguridad de sistemas	Aplica	Existe tanto desarrollo de software interno como externalizado.
14.2.9 Pruebas de aceptación de sistemas	Aplica	Existe tanto desarrollo de software interno como externalizado.
14.3.1 Protección de los datos de prueba	Aplica	Existe tanto desarrollo de software interno como externalizado.
15. RELACIÓN CON PROVEEDORES		
15.1.1 Política de seguridad de la información en las relaciones con los proveedores	Aplica	Hay proveedores que tratan información de la organización.
15.1.2 Requisitos de seguridad en contratos con terceros	Aplica	Hay proveedores que tratan información de la organización.
15.1.3 Cadena de suministros de tecnología de la información y de las comunicaciones	Aplica	La organización compra productos TIC a proveedores.
15.2.1 Control y revisión de la provisión de servicios del proveedor	Aplica	Existen servicios ofrecidos por proveedores como el de copias de respaldo.
15.2.2 Gestión de cambios en la provisión del servicio del proveedor	Aplica	Existen servicios ofrecidos por proveedores como el de copias de respaldo.
16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN		
16.1.1 Responsabilidades y procedimientos	Aplica	Pueden ocurrir incidentes/eventos de seguridad de la información que se deben gestionar.
16.1.2 Notificación de los eventos de seguridad de la	Aplica	Pueden ocurrir incidentes/eventos de seguridad de la información que se deben gestionar.

información		
16.1.3 Notificación de puntos débiles de la seguridad	Aplica	Pueden ocurrir incidentes/eventos de seguridad de la información que se deben gestionar.
16.1.4 Evaluación y decisión sobre los eventos de seguridad de información	Aplica	Pueden ocurrir incidentes/eventos de seguridad de la información que se deben gestionar.
16.1.5 Respuesta a incidentes de seguridad de la información	Aplica	Pueden ocurrir incidentes/eventos de seguridad de la información que se deben gestionar.
16.1.6 Aprendizaje de los incidentes de seguridad de la información	Aplica	Pueden ocurrir incidentes/eventos de seguridad de la información y se debería aprender de los mismos para que no vuelvan a ocurrir o gestionarlos con mayor efectividad.
16.1.7 Recopilación de evidencias	Aplica	Pueden ocurrir incidentes/eventos de seguridad de la información y se tiene que recopilar evidencias para conocer la causa de los mismos.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO		
17.1.1 Planificación de la continuidad de la seguridad de la información	Aplica	Se debe asegurar los requisitos de seguridad de la información en situaciones de crisis o desastres.
17.1.2 Implementar la continuidad de la seguridad de la información	Aplica	Se debe asegurar los requisitos de seguridad de la información en situaciones de crisis o desastres.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Aplica	Se debe asegurar los requisitos de seguridad de la información en situaciones de crisis o desastres.
17.2.1 Disponibilidad de los recursos de tratamiento de la información	Aplica	Se debe asegurar la disponibilidad de los sistemas de información en situaciones de crisis o desastres.
18. CUMPLIMIENTO		
18.1.1 Identificación de la legislación	Aplica	Se debe identificar la legislación aplicable para evitar incumplimientos de las obligaciones legales

aplicable y de los requisitos contractuales		relativas a la seguridad de la información.
18.1.2 Derechos de propiedad intelectual (DPI)	Aplica	Se debe cumplir con los derechos de propiedad intelectual.
18.1.3 Protección de los registros de la organización	Aplica	Existen registros contables, logs de las bases de datos, de auditoría, etc. que se deben proteger.
18.1.4 Protección y privacidad de la información de carácter personal	Aplica	La organización trata datos de carácter personal y hay legislación nacional aplicable.
18.1.5 Regulación de los controles criptográficos	Aplica	La organización usa controles criptográficos.
18.2.1 Revisión independiente de la seguridad de la información	Aplica	Se deben realizar revisiones independientes periódicas de seguridad de la información para implantar un SGSI.
18.2.2 Cumplimiento de las políticas y normas de seguridad	Aplica	Se debe comprobar el cumplimiento de las políticas y normas de seguridad.
18.2.3 Comprobación del cumplimiento técnico	Aplica	Se debe realizar revisiones de las aplicaciones e infraestructura de la organización para ver si cumple con la normativa de seguridad establecida.

4. ANÁLISIS DE RIESGOS

Se va a realizar el análisis de riesgos teniendo en cuenta la metodología del apartado "3.2.6 Metodología de Análisis de Riesgos" para identificar los riesgos más relevantes a los que se encuentran sometidos los activos de la organización, y teniendo en cuenta las medidas de seguridad que ya estén implantadas previamente. De esta manera, la organización podrá conocer el nivel de riesgo actual al que se encuentran sometidos sus activos de información incluidos dentro del alcance del SGSI.

4.1 MODELO DE VALOR

4.1.1 IDENTIFICACIÓN DE LOS ACTIVOS

Se considera activo a aquel componente o funcionalidad del sistema de información de la organización que se debe proteger de riesgos y amenazas para asegurar el buen funcionamiento de su negocio.

Teniendo esto en cuenta, a continuación, se muestran los activos identificados en la organización que son más relevantes para poder afrontar la complejidad del análisis, clasificados según su naturaleza como establece la metodología MAGERIT [8].

Además, se ha asignado un propietario de los mismos que serán el que ayuda a la valoración del activo según la importancia que tenga dentro de la organización.

ÁMBITO	CÓDIGO	ACTIVO	UBICACIÓN	PROPIETARIO
[I] Información / Datos	[I.1]	Base de datos de RRHH	CPD	Jefe RHHH
	[I.2]	Base de datos con información de interés primordial para negocio (clientes, pólizas, asistencias)	CPD	Dirección General
	[I.3]	Base de datos con las grabaciones de voz del Call Center	CPD	Jefe Comercial
	[I.4]	Base de datos con información de configuración y gestión inventario y seguridad	CPD	Jefe TI y procesos
[S] Servicios	[S.1]	Servicio de venta de pólizas online	N/A	Jefe Comercial
	[S.2]	Servicio del Call Center de asistencias al usuario	N/A	Jefe Comercial

[K] Claves Criptográficas	[K.1]	Claves para el uso de la VPN para el acceso remoto	CPD	Jefe TI y procesos
[SW] Aplicaciones	[SW.1]	Sistema operativo	Edificios 1 y 2 (en equipos y servidores)	Jefe TI y procesos
	[SW.2]	Pack de ofimática	Edificios 1 y 2 (en equipos y servidores)	Jefe TI y procesos
	[SW.3]	Antivirus	Edificios 1 y 2 (en equipos y servidores)	Jefe TI y procesos
	[SW.4]	Sistemas de gestión de pólizas y otros trámites necesarios para negocio	CPD	Dirección General
	[SW.5]	Plataforma operativa de atención al cliente (asistencia en carretera, viaje, sanitaria, etc.)	CPD	Jefe Comercial
	[SW.6]	Web comercial y portal para contratar pólizas	CPD	Dirección General
	[SW.7]	Correo electrónico	Edificios 1 y 2	Dirección General
[HW] Equipos	[HW.1]	Servidores que se encuentran en el CPD (servidor de negocio, de correo, de configuración y gestión de la seguridad, de RRHH, de DA, mostrados en el diagrama de red)	Edificio 1 (planta baja CPD)	Jefe TI y procesos
	[HW.2]	PC del puesto de usuario	Edificios 1 y 2 (planta 1 y Call Center)	El empleado propietario del mismo
	[HW.3]	Portátil	Edificio 1 (planta1)	El empleado propietario del mismo
	[HW.4]	Teléfonos VoIP y centralita	Edificio 2 (Call Center)	Jefe TI y procesos
	[HW.5]	Firewalls	CPD	Jefe TI y procesos

	[HW.6]	Routers	CPD y sala de racks del Edificio 2	Jefe TI y procesos
	[HW.7]	Switches	CPD y sala de racks del Edificio 2	Jefe TI y procesos
[COM] Comunicaciones	[COM.1]	Cableado de datos de VoIP	Líneas de comunicación en el Edificio 2	Jefe TI y procesos
	[COM.2]	Internet	Líneas de comunicación distribuidas por ambos edificios	Jefe TI y procesos
[AUX] Equipamiento auxiliar	[AUX.1]	UPS	Edificio 1 y 2	Jefe TI y procesos
	[AUX.2]	Generadores eléctricos	Edificio 1 y 2	Jefe TI y procesos
	[AUX.3]	Equipos de climatización	Edificio 1 (en la sala del CPD y en el cuarto del generador eléctrico)	Jefe TI y procesos
[SS] Servicios Subcontratados	[SS.1]	Servicio de respaldo externalizados en la nube (solo información de interés alto para negocio)	En la nube del proveedor	Jefe TI y procesos
[L] Instalaciones	[L.1]	Centro de datos (CPD)	Edificio 1 (en la sala del CPD)	Jefe TI y procesos
	[L.2]	Cuarto de racks	Edificio 2 donde se encuentran equipos con conexión al CPD	Jefe TI y procesos
	[L.3]	Recinto	Incluye el Edificio 1 y el Edificio 2	Dirección General
[P] Personal	[P.1]	Empleados Edificio 1	Edificio 1 (planta 1)	Dirección General
	[P.2]	Empleados del Call Center en el Edificio 2	Edificio 2 (Call Center)	Dirección General
	[P.3]	Empleados de seguridad privada a la entrada del recinto	Control de Acceso del recinto	Dirección General

Tabla 5. Inventario de activos

4.1.2 DEPENDENCIAS DE LOS ACTIVOS

Una vez identificados los activos, se tienen que tener en cuenta las dependencias que existen entre ellos. En este análisis de riesgos no se ha teniendo en cuenta las dependencias aquí mostradas para no añadir más complejidad al análisis, aunque se puede ver que un **riesgo alto en los activos inferiores tendrá impacto en los activos superiores**, siendo el personal transversal a todos los activos.

A continuación se muestra de manera generalista las dependencias que existen entre las distintas categorías de activos:

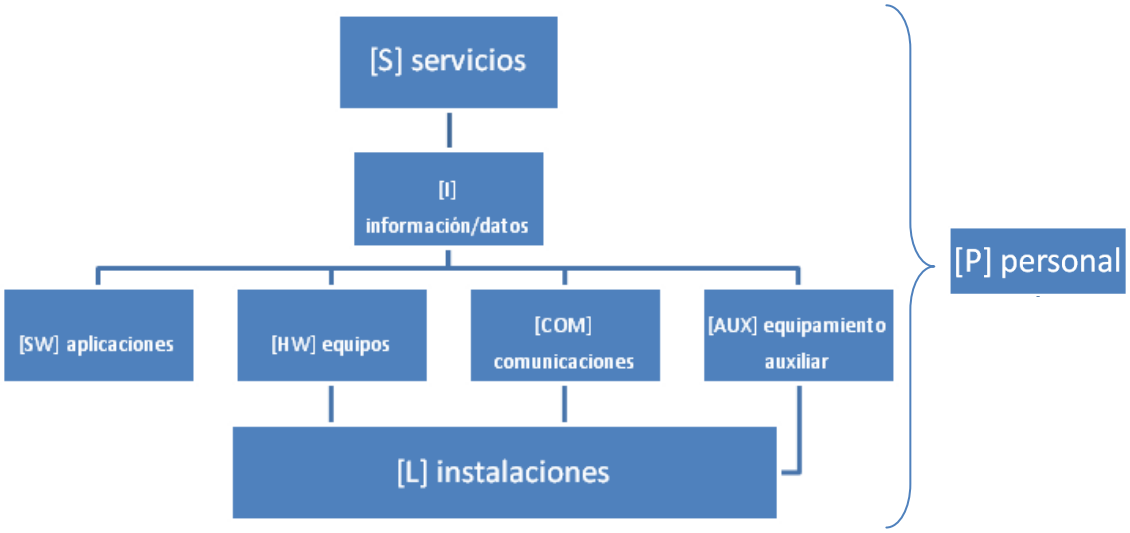

Fig. 6: Dependencias entre activos

4.1.3 VALORACIÓN DE LOS ACTIVOS

Teniendo en cuenta los pasos y las tablas 1 y 2 expuestas en el punto "3.2.6 Metodología de Análisis de Riesgos", se procede a valorar los activos cuantitativamente, y a identificar qué dimensiones de seguridad resultan más críticas si se materializase una amenaza en dicho activo:

ÁMBITO	CÓD.	ACTIVO	VALORACIÓN ACTIVO	VALORACIÓN CUANTITATIVA	[C]	[I]	[D]	[A]	[T]
[I] Información / Datos	[I.1]	Base de datos de RRHH	A	€ 100.000,00	8	9	7	8	8
	[I.2]	Base de datos con información de interés primordial para negocio (clientes, pólizas, asistencias)	MA	€ 350.000,00	9	9	9	9	9
	[I.3]	Base de datos con las grabaciones de voz del Call Center	MA	€ 350.000,00	6	7	6	8	8
	[I.4]	Base de datos con información de configuración y gestión inventario y seguridad	A	€ 100.000,00	6	7	7	9	9
[S] Servicios	[S.1]	Servicio de venta de pólizas online	MA	€ 350.000,00	6	8	9	9	9
	[S.2]	Servicio del Call Center de asistencias al usuario	MA	€ 350.000,00	6	8	9	8	8
[K] Claves Criptográficas	[K.1]	Claves para el uso de la VPN para el acceso remoto	B	€ 10.000,00	8	8	7		
[SW] Aplicaciones	[SW.1]	Sistema operativo	MB	€ 1.000,00	3	5	5		
	[SW.2]	Pack de ofimática	MB	€ 1.000,00	3	5	5		
	[SW.3]	Antivirus	MB	€ 1.000,00	3	5	7		
	[SW.4]	Sistemas de gestión de pólizas y otros trámites necesarios para negocio	M	€ 50.000,00	6	8	9		
	[SW.5]	Plataforma operativa de atención al cliente (en carretera, viaje, sanitaria)	M	€ 50.000,00	6	8	9		
	[SW.6]	Web comercial, para contratar pólizas	M	€ 50.000,00	8	9	9		
	[SW.7]	Correo electrónico	M	€ 50.000,00	3	6	6		
[HW] Equipos	[HW.1]	Servidores que se encuentran en el CPD (servidor de negocio, de correo, de configuración y gestión de la seguridad, de RRHH, de DA, mostrados en el	M	€ 50.000,00	8	7	9		

		diagrama de red)							
	[HW.2]	Puesto fijo personal	B	€ 10.000,00	8	4	2		
	[HW.3]	Portátil	B	€ 10.000,00	8	5	3		
	[HW.4]	Teléfonos VoIP y centralita	B	€ 10.000,00	6	3	8		
	[HW.5]	Firewalls	M	€ 50.000,00	8	8	9		
	[HW.6]	Routers	MB	€ 1.000,00	3	2	7		
	[HW.7]	Switches	MB	€ 1.000,00	6	5	6		
[COM] Comunicaciones	[COM.1]	Cableado de datos de VoIP	B	€ 10.000,00	6	0	8		
	[COM.2]	Internet	M	€ 50.000,00	8	5	9		
[AUX] Equipamiento auxiliar	[AUX.1]	UPS	B	€ 10.000,00	0	0	7		
	[AUX.2]	Generadores eléctricos	B	€ 10.000,00	0	0	7		
	[AUX.3]	Equipos de climatización	B	€ 10.000,00	0	0	8		
[SS] Servicios Subcontratados	[SS.1]	Servicio de respaldo externalizados en la nube	M	€ 50.000,00	8	8	9		
[L] Instalaciones	[L.1]	Centro de datos (CPD)	M	€ 50.000,00	6	5	9		
	[L.2]	Cuarto de rack	MB	€ 1.000,00	4	3	5		
	[L.3]	Recinto	MA	€ 350.000,00	6	5	9		
[P] Personal	[P.1]	Empleados del Edificio 1	A	€ 100.000,00	8	5	8		
	[P.2]	Empleados del Call Center en el Edificio 2	A	€ 100.000,00	4	4	9		
	[P.3]	Empleados de seguridad privada a la entrada del recinto	B	€ 10.000,00	3	3	7		

4.2 MAPA DE RIESGOS

4.2.1 IDENTIFICACIÓN DE LAS AMENAZAS

Después de realizar la valoración de activos, se procederá a considerar las amenazas que pueden producir mayor daño. En el análisis de riesgos de este SGSI, se han clasificado las amenazas potenciales por su origen, y después se ha valorado a qué activos pueden afectar y qué dimensiones de seguridad del activo pueden verse afectadas si se materializan [8]. La descripción de los códigos identificativos de la amenaza y la tabla con las amenazas se encuentran a continuación:

- [N] Desastres naturales
- [I] De origen industrial
- [E] Errores y fallos no intencionados
- [A] Ataques intencionados

Código	Amenaza	Tipos de activos que pueden ser afectados	[C]	[I]	[D]	[A]	[T]
[N.1]	Fuego (origen natural)	[HW],[AUX],[L]			x		
[N.2]	Daños por agua (origen natural)	[HW],[AUX],[L]			x		
[N.3]	Desastres naturales	[HW],[AUX],[L]			x		
[I.1]	Fuego (origen industrial)	[HW],[AUX],[L]			x		
[I.2]	Daños por agua (origen industrial)	[HW],[AUX],[L]			x		
[I.3]	Contaminación mecánica (vibraciones, suciedad...)	[HW],[AUX]			x		
[I.4]	Contaminación electromagnética	[HW],[AUX]			x		
[I.5]	Avería de origen físico o lógico	[SW],[HW],[AUX]			x		
[I.6]	Corte del suministro eléctrico	[HW],[AUX]			x		
[I.7]	Condiciones inadecuadas de temperatura o humedad	[HW],[AUX]			x		
[I.8]	Fallo de servicios de comunicaciones	[COM]			x		
[I.9]	Interrupción de otros servicios y suministros esenciales	[AUX]			x		
[I.11]	Emanaciones electromagnéticas	[HW],[AUX],[L]	x				

[I.12]	Otros desastres industriales (fluctuaciones eléctricas, derrumbes, etc.)	[HW],[AUX],[L]			x		
[E.1]	Errores de los usuarios	[I],[K],[S],[SW]	x	x	x		
[E.2]	Errores del administrador	[I],[K],[S],[SW],[HW],[COM]	x	x	x		
[E.3]	Errores de monitorización (log)	[I]		x			x
[E.4]	Errores de configuración	[I]		x			
[E.7]	Deficiencias en la organización	[P]			x		
[E.8]	Difusión de software dañino	[SW]	x	x	x		
[E.9]	Errores de [re-] encaminamiento	[S],[SW],[COM]	x				
[E.10]	Errores de secuencia	[S],[SW],[COM]		x			
[E.15]	Alteración accidental de la información	[I],[K],[S],[SW],[COM],[L]		x			
[E.18]	Destrucción de información	[I],[K],[S],[SW],[COM],[L]			x		
[E.19]	Fugas de información	[I],[K],[S],[SW],[COM],[L],[P]	x				
[E.20]	Vulnerabilidades de los programas (software)	[SW]	x	x	x		
[E.21]	Errores de mantenimiento/actualización de programas (software)	[SW]		x	x		
[E.23]	Errores de mantenimiento/actualización de equipos (hardware)	[HW],[AUX]			x		
[E.24]	Caída del sistema por agotamiento de recursos	[S],[HW],[COM]			x		
[E.25]	Pérdida de equipos	[HW],[AUX]	x		x		
E.28]	Indisponibilidad del personal (enfermedad)	[P]			x		
[A.3]	Manipulación de los registros de actividad (log)	[I]		x			x
[A.4]	Manipulación de la configuración	[I]	x	x		x	
[A.5]	Suplantación de la	[I],[K],[S],[SW],[COM]	x	x		x	

	identidad del usuario						
[A.6]	Abuso de privilegios de acceso	[I],[K],[S],[SW],[HW],[COM]	x	x	x		
[A.7]	Uso no previsto	[S],[SW],[HW],[COM],[AUX],[L]	x	x	x		
[A.8]	Difusión de software dañino (intencionadamente)	[SW]	x	x	x		
[A.9]	[Re-]encaminamiento	[S],[SW],[COM]	x				
[A.10]	Alteración de secuencia	[S],[SW],[COM]		x			
[A.11]	Acceso no autorizado	[I],[K],[S],[SW],[HW],[COM], [AUX],[L]	x	x			
[A.12]	Análisis de tráfico	[COM]	x				
[A.13]	Repudio	[I],[S]		x			x
[A.14]	Interceptación de información (escucha)	[COM]	x				
[A.15]	Modificación deliberada de la información	[I],[K],[S],[SW],[COM],[L]		x			
[A.18]	Destrucción de información	[I],[K],[S],[SW],[L]			x		
[A.19]	Divulgación de información	[I],[K],[S],[SW],[COM],[L]	x				
[A.22]	Manipulación de programas	[SW]	x	x	x		
[A.23]	Manipulación de los equipos	[HW],[AUX]	x		x		
[A.24]	Denegación de servicio	[S],[HW],[COM]			x		
[A.25]	Robo	[HW],[AUX]	x		x		
[A.26]	Ataque destructivo	[HW],[AUX],[L]			x		
[A.27]	Ocupación enemiga	[L]	x		x		
[A.28]	Indisponibilidad del personal (ausencia deliberada del puesto de trabajo)	[P]			x		
[A.29]	Extorsión	[P]	x	x	x		
[A.30]	Ingeniería social (picaresca)	[P]	x	x	x		

Tabla 6. Amenazas potenciales y dimensiones a las que afectan

4.2.2 VALORACIÓN DE LAS AMENAZAS POR TIPO DE ACTIVOS

Considerando las amenazas que pueden afectar a los activos identificados anteriormente, se procede a evaluar el nivel de degradación, probabilidad e impacto causado por una amenaza cuando se materializa sobre un activo, para después calcular el riesgo al que está expuesto dicho activo. Los resultados se pueden encontrar en el Anexo.

Impacto = Valoración de la dimensión de seguridad del activo * Degradación

Riesgo = Impacto * Probabilidad * Valor Activo (€)

4.3 CÁLCULO DE NIVEL DE RIESGO

Para determinar el nivel de riesgo al que está expuesto un activo después de haber realizado el cálculo de riesgo al que están sometidos, se ha teniendo en cuenta la siguiente tabla:

NIVEL DE RIESGO	RANGO CUANTITATIVO (€)
Alto	mayor que 10.000
Medio	10.000 - 5.000
Bajo	5.000 - 1.000
Mínimo	1.000 - 100
Despreciable	menor que 100

Tabla 7. Clasificación del Nivel de Riesgo de los Activos

La organización considera aprobar y determinar el nivel de riesgo residual en todos los riesgos de activos con un valor menor al nivel de riesgo medio, es decir, menor de 5.000 €, por lo que 18 activos por debajo del nivel medio no tendrán un plan de tratamiento del riesgo.

Por otro lado, 14 activos de la organización si tendrán asociados planes de tratamiento de riesgos, donde los riesgos de nivel alto asociados a 9 activos, serán tratados con prioridad alta, y los riesgos de nivel medio asociados a 5 activos, serán tratados con prioridad media y los riesgos con nivel por debajo del medio, serán asumidos por la organización estando en constante monitorización y revisión periódica.

Los resultados obtenidos han sido los siguientes:

CÓDIGO	ACTIVO	RIESGO DEL ACTIVO	PROPIETARIO DEL RIESGO
[S.2]	Servicio del Call Center de asistencias al usuario	127.917,81 €	Supervisor del call center
[I.2]	Base de datos con información de interés primordial para negocio (clientes, pólizas, asistencias)	56.095,89 €	Jefe TI y procesos
[S.1]	Servicio de venta de pólizas online	53.305,48 €	Jefe TI y procesos
[I.3]	Base de datos con las grabaciones de voz del Call Center	43.678,08 €	Jefe TI y procesos
[P.1]	Empleados del Edificio 1	22.136,99 €	Jefe RRHH
[L.3]	Recinto	20.616,44 €	Jefe Operaciones
[HW.5]	Firewalls	13.393,15 €	Jefe TI y procesos
[HW.1]	Servidores que se encuentran en el CPD (servidor de negocio, de correo, de configuración y gestión de la seguridad, de RRHH, de DA, mostrados en el diagrama de red)	12.691,78 €	Jefe TI y procesos
[I.4]	Base de datos con información de configuración y gestión inventario y seguridad	12.150,68 €	Jefe TI y procesos
[I.1]	Base de datos de RRHH	10.191,78 €	Jefe TI y procesos
[SW.6]	Web comercial, para contratar pólizas	8.534,25 €	Jefe TI y procesos
[L.1]	Centro de datos (CPD)	7.808,22 €	Jefe TI y procesos
[SW.4]	Sistemas de gestión de pólizas y otros trámites necesarios para negocio	7.356,16 €	Jefe TI y procesos
[SW.5]	Plataforma operativa de atención al cliente (en carretera, viaje, sanitaria)	7.356,16 €	Jefe TI y procesos
[HW.3]	Portátil	2.491,51 €	Jefe TI y procesos
[COM.2]	Internet	2.301,37 €	Jefe TI y procesos
[HW.4]	Teléfonos VoIP y centralita	1.711,78 €	Jefe TI y procesos
[HW.2]	Puesto fijo personal	1.649,32 €	Jefe TI y procesos
[P.2]	Empleados del Call Center en el Edificio 2	1.632,88 €	Jefe RRHH
[P.3]	Empleados de seguridad privada a la entrada del recinto	802,74 €	Jefe TI y procesos
[HW.6]	Routers	309,62 €	Jefe TI y procesos

[HW.7]	Switches	302,96 €	Jefe TI y procesos
[COM.1]	Cableado de datos de VoIP	268,49 €	Jefe TI y procesos
[K.1]	Claves para el uso de la VPN para el acceso remoto	175,34 €	Jefe TI y procesos
[SW.7]	Correo electrónico	107,18 €	Jefe TI y procesos
[SW.3]	Antivirus	97,89 €	Jefe TI y procesos
[AUX.3]	Equipos de climatización	92,05 €	Jefe TI y procesos y el de Operaciones
[SW.1]	Sistema operativo	75,42 €	Jefe TI y procesos
[SW.2]	Pack de ofimática	56,52 €	Jefe TI y procesos
[AUX.1]	UPS	42,19 €	Jefe TI y procesos y el de Operaciones
[AUX.2]	Generadores eléctricos	42,19 €	Jefe TI y procesos y el de Operaciones
[L.2]	Cuarto de rack	36,16 €	Jefe TI y procesos

Tabla 8. Riesgo calculado de los activos en la organización

5. PLANES DE MEJORA

En el presente apartado se llevará a cabo la Gestión de Riesgos, describiéndose los proyectos con sus respectivas salvaguardas o planes de tratamiento del riesgo de los activos que la organización ha decidido no asumir y por tanto, se deben tratar. Dichos planes pretenden que los riesgos sean atajados o reducidos a niveles aceptables por la organización.

Además, en esta etapa se debe informar al personal responsable del activo que se va a tratar, de las amenazas a las que está expuesto y las salvaguardas que se deciden implantar para minimizar el riesgo asociado. Muchas de las salvaguardas enmarcadas en los proyectos, son de bajo coste, pero con un importante impacto en la gestión del riesgo, y se pretenden implantar a lo largo de un año, ya que en el 2020 la organización sufrirá la primera revisión de su SGSI.

Cabe mencionar, que, aunque principalmente se hace hincapié en gestionar el riesgo de los activos que superan el umbral asumible por la organización, la implantación de los proyectos hará que muchos de los activos restantes, dependientes unos de otros, también se vean afectados por ello y reduzcan su nivel de riesgo.

5.1 IDENTIFICACIÓN DE LAS MEJORAS NECESARIAS

A continuación, se describen las mejoras identificadas basadas en las amenazas a las que se pretende hacer frente para mitigar los principales riesgos no asumidos por la organización, los activos bajo tratamiento que se van a ver beneficiados por los proyectos, y los dominios de seguridad de la ISO 27002 que mejoran sustancialmente.

Más adelante, en el apartado 5.2 se describirán los proyectos y su planificación.

IDENTIFICACIÓN DE MEJORAS	PROYECTOS DE MEJORA PROPUESTOS	AMENAZAS IDENTIFICADAS A LAS QUE HACE FRENTE	ACTIVOS A LOS QUE AFECTA (asociados a nivel alto y medio *Tabla 6)*	RIESGO A TRATAR	DOMINIOS QUE MEJORAN
Revisar las políticas de seguridad de la información y los procedimientos de gestión de los controles de seguridad de la información que son de aplicabilidad.	**PRO-1:** Revisión de las políticas de seguridad de la información y los procedimientos de gestión de los controles de seguridad de la información que son de aplicabilidad	[E.1] Errores de los usuarios, [E.2] Errores del administrador, [E.4] Errores de configuración, [E.21] Errores de mantenimiento/actualización de programas (software), [E.23] Errores de mantenimiento/actualización de equipos (hardware), [A.7] Uso no previsto, [A.19] Divulgación de información	Afecta a todos los activos que se quieren tratar en la tabla de riesgos altos y médicos identificados: [S.2], [S.2], [S.1], [I.3], [P.1], [L.3], [HW.5], [HW.1], [I.4], [I.1], [SW.6], [L.1], [SW.4], [SW.5].	Mitiga y trata los riesgos asociados a la organización y gestión de la seguridad de la información (personas, sistemas, servicios…), mejorando su gobernanza	5. Políticas de seguridad de la información. Además, los dominios principales que mejorarían si se elaborasen los procedimientos que se han identificado que faltan durante el análisis diferencial: 7. Seguridad relativa a los RRHH (antes, durante y después del empleo, planes de formación…), 8. Gestión de activos, 9. Control de acceso, 10. Criptografía, 12. Seguridad de las operaciones, 14. Adquisición, desarrollo y mantenimiento de los SI, 16. Gestión de incidentes, 18. Cumplimiento
Mejora en la gestión y el control de la seguridad de la información.	**PRO-2:** Implantación de Comités de Seguridad	[E.7] Deficiencias en la organización	Afecta a todos los activos que se quieren tratar en la tabla de riesgos altos y médicos identificados: [S.2], [S.2], [S.1], [I.3], [P.1], [L.3], [HW.5], [HW.1], [I.4], [I.1], [SW.6], [L.1], [SW.4], [SW.5].	Mitiga y trata el riesgo de la mala gestión de los activos a tratar haciendo seguimiento de los mismos y mitiga posibles incumplimientos normativos en materia de	6. Organización de la seguridad de la información, 18. Cumplimiento (18.2.2 Cumplimiento de las políticas y normas de seguridad)

				seguridad.	
Mejora en la gestión de la seguridad del servicio Call Center	**PRO-3:** Plan de Externalización del Call Center	Se ha identificado que el activo con mayor riesgo es el servicio de Call Center. La empresa está en crecimiento y cualquier indisponibilidad en el servicio (ya sea de comunicaciones, de personal, de infraestructura, etc.) puede afectar a la pérdida de clientes. La mayor amenaza a la que hace frente es a la [E.24] Caída del sistema por agotamiento de recursos.	[I.3] Base de datos con las grabaciones de voz del Call Center, [S.2] Servicio del Call Center de asistencias al usuario, [SW.5] Plataforma operativa de atención al cliente (asistencia en carretera, viaje, sanitaria, etc.).	Mitiga y trata el riesgo de indisponibilidad y calidad en los servicios asociados al Call Center debido al crecimiento que está experimentando la organización	12. Seguridad de las operaciones, 14. Adquisición, desarrollo y mantenimiento de los S.I, 17. Aspectos de S.I para la gestión de la continuidad de negocio, 18. Cumplimiento
Mejora en la seguridad de los sistemas de información (en este caso servidores), que tratan o almacenan información.	**PRO-4:** Plan de Bastionado de Servidores	[E.8] Difusión de software dañino,[E.19] Fugas de información, [E.23] Errores de mantenimiento/actualización de equipos (hardware), [A.6] Abuso de privilegios de acceso, [A.7] Uso no previsto, [A.11] Acceso no autorizado, [A.23] Manipulación de los equipos,	[HW.1] Servidores que se encuentran en el CPD con información (servidor de info. Clave para negocio, de correo, de configuración y gestión de la seguridad, de RRHH, de DA)	Mitiga el riesgo de ataque en los servidores que alojan información clave para organización	12. Seguridad de las operaciones

Mejora en la destrucción de documentos y soportes obsoletos con información confidencial	**PRO-5:** Plan de Externalización del servicio de destrucción de la información	[E.19] Fugas de información, [A.5] Suplantación de la identidad del usuario, [A.15] Modificación deliberada de la información, [A.19] Divulgación de información	[I.2] BBDD con información de interés primordial para negocio (clientes, pólizas, asistencias...), [I.3] BBDD con las grabaciones de voz del Call Center, [I.4] BBDD con información de configuración y gestión inventario y seguridad, [I.1] BBDD RRHH, [HW.5] Firewalls, [HW.1] Servidores que se encuentran en el CPD.	Mitiga el riesgo de fuga de información alojada en sistemas obsoletos que tienen en el almacén o información en papel que no sirve y tienen los empleados en archivos o encima de sus mesas	8. Gestión de activos
Mejora en la seguridad de la información que tratan, almacenan o transmiten los sistemas de información (aplicaciones e infraestructuras) publicados en DMZ	**PRO-6:** Plan de Revisiones Técnicas de Seguridad de la DMZ	[E.8] Difusión de software dañino, [E.19] Fugas de información, [E.20] Vulnerabilidades de los programas (software), [A.8] Difusión de software dañino (intencionadamente), [A.24] Denegación de servicio	[SW.6] Web comercial y portal para contratar pólizas.	Mitiga y trata riesgos asociados a las vulnerabilidades presentes en aplicaciones críticas de negocio	14. Adquisición, desarrollo y mantenimiento de los S.I., 18. Cumplimiento (18.2.3 Comprobación del cumplimiento técnico)

Concienciar y formar al personal en seguridad de la información	**PRO-7:** Planes de Concienciación en Seguridad y Formación	[E.1] Errores de los usuarios, [E.2] Errores del administrador, [E.4] Errores de configuración, [E.7] Deficiencias en la organización, [E.21] Errores de mantenimiento/actualización de programas (software), [E.23] Errores de mantenimiento/actualización de equipos (hardware), [A.7] Uso no previsto, [A.19] Divulgación de información, [A.30] Ingeniería social (picaresca)	[P.1] Empleados del Edificio 1	Mitiga y trata riesgos asociados a errores humanos	7. Seguridad relativa a los recursos humanos
Mejoras de seguridad en el CPD	**PRO-8:** Plan de mejora de la seguridad del CPD	[N.1] Fuego (origen natural), [N.2] Daños por agua (origen natural), [N.3] Desastres naturales, [I.6] Corte del suministro eléctrico, [A.5] Suplantación de la identidad del usuario, [I.1] Fuego (origen industrial), [I.2] Daños por agua (origen industrial), [I.7] Condiciones inadecuadas de temperatura o humedad, [I.12] Otros	[HW.1] Servidores que se encuentran en el CPD, [L.1] Centro de datos (CPD), [I.2] BBDD con información de interés primordial para negocio (clientes, pólizas, asistencias...), [I.3] BBDD con las grabaciones de voz del Call Center, [I.4] BBDD con información de configuración y gestión inventario y seguridad, [I.1]	Mitiga y trata riesgos de indisponibilidad en los servidores, sistemas e infraestructuras de la organización incluidos en la tabla de riesgos a tratar	9. Control de acceso, 11. Seguridad física y del entorno, 17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio, 18. Cumplimiento

		desastres industriales (fluctuaciones eléctricas, derrumbes, etc.), [E.24] Caída del sistema por agotamiento de recursos, [A.11] Acceso no autorizado, [A.18]Destrucción de información, [A.23] Manipulación de los equipos, [A.24] Denegación de servicio, [A.25] Robo, [A.26] Ataque destructivo.	BBDD RRHH, [SW.6] Sistemas de gestión de pólizas y otros trámites necesarios para negocio, [SW.4] Sistemas de gestión de pólizas y otros trámites necesarios para negocio, [SW.5] Plataforma operativa de atención al cliente (en carretera, viaje, sanitaria), [S.1] Servicio de venta de pólizas online y [S.2] Servicio del Call Center de asistencias al usuario.		
Mejoras en la continuidad de negocio	**PRO-9:** Plan de Continuidad de Negocio	[N.1] Fuego (origen natural), [N.2] Daños por agua (origen natural), [N.3] Desastres naturales, [I.6] Corte del suministro eléctrico, [A.5] Suplantación de la identidad del usuario, [I.1] Fuego (origen industrial), [I.2] Daños por agua (origen industrial), [I.7] Condiciones inadecuadas de temperatura o humedad, [I.12] Otros desastres industriales (fluctuaciones eléctricas,	Afecta a todos los activos que se quieren tratar en la tabla de riesgos altos y médicos identificados: [S.2], [S.2], [S.1], [I.3], [P.1], [L.3], [HW.5], [HW.1], [I.4], [I.1], [SW.6], [L.1], [SW.4], [SW.5].	Mitiga y trata riesgos de indisponibilidad en todos los activos de la organización incluidos en la tabla de riesgos a tratar	11. Seguridad física y del entorno, 17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio, 18. Cumplimiento

		derrumbes, etc.), [E.24] Caída del sistema por agotamiento de recursos, [A.11] Acceso no autorizado, [A.18]Destrucción de información, [A.23] Manipulación de los equipos, [A.24] Denegación de servicio, [A.25] Robo, [A.26] Ataque destructivo, [E.28] Indisponibilidad del personal (enfermedad), [A.28] Indisponibilidad del personal (ausencia deliberada del puesto de trabajo).			

5.2 DESARROLLO DEL PLAN DE MEJORAS

A continuación, se describen los proyectos propuestos de mejora para gestionar los activos con mayor riesgo encontrados.

5.2.1 PRO-1: Revisión de las políticas de seguridad de la información y los procedimientos de gestión de los controles de seguridad de la información que son de aplicabilidad.

DESCRIPCIÓN:

Durante el análisis diferencial efectuado, se ha detectado que las políticas de seguridad de la información no tienen establecidas periódicamente una revisión, ni cuando se producen cambios organizativos. Por eso se ha decidido establecer un plan de revisiones cada dos años, donde la Dirección y cada uno de los responsables asignados, tendrán que mantenerlas actualizadas y detectar posibles oportunidades de mejora.

Por otro lado, existen procedimientos definidos dentro de la organización para la adecuada gestión de los controles de seguridad, pero se ha detectado que también faltan muchos otros procedimientos por definir que permitirán la mejora de la seguridad de la información.

A continuación, se detallan los procedimientos de los controles que se han echado en falta y que deberían elaborarse:

- Procedimiento de Gestión de Incidentes.
- Procedimiento para la Gestión de Cambios.
- Procedimiento para garantizar el cumplimiento de requisitos legales sobre el uso de materiales con Derechos de Propiedad Intelectual.
- Procedimiento de uso de los Controles Criptográficos
- Procedimiento para la Gestión de los RRHH.
- Procedimiento formal de revisión periódica de accesos y de control de acceso.

A parte de la elaboración de los procedimientos anteriormente mencionados, se debe difundir a los empleados el procedimiento elaborado recientemente sobre el uso aceptable de activos para que tengan conocimiento del mismo y lo firmen.

Por otro lado, para gestionar de manera adecuada algunas de las amenazas relativas a los errores de configuración, se debe contar con guías o procedimientos adicionales con la configuración correcta de los sistemas, elementos de red, etc., de los cuales harán uso un personal específico.

PLANIFICACIÓN:

Revisión de las Políticas de Seguridad de la Información: cada 2 años.

Elaboración de los Procedimientos que faltan para la gestión adecuada de los controles: 6 meses.

COSTE:

El principal coste va asociado al tiempo invertido en la revisión y elaboración de procedimientos traducido en el sueldo de los integrantes de la Dirección y de los responsables de elaborar los procedimientos para la gestión de los controles. Se va a contar con la participación de un responsable de la Dirección, donde se destinará el 15% del sueldo mensual para llevar a cabo este proyecto, más tres personas responsables pertenecientes a TI, RRH y Legal, los cuales participarán en la elaboración de los procedimientos, destinando entre los tres un total del 50% de un sueldo mensual medio de un responsable de área. Dicho lo anterior, el coste aproximado calculado es de aproximadamente 19.000 €.

5.2.2 PRO-2: Implantación de Comités de Seguridad

DESCRIPCIÓN:

Este proyecto pretende establecer la realización periódica de Comités de Seguridad de la Información donde acudan las partes involucradas en el SGSI, para debatir, presentar y dar seguimiento al estado de los indicadores que se establezcan como mediciones de cumplimiento del SGSI, pudiendo identificar la evolución y mejora alcanzada.

En el primer Comité se establecerán formalmente los roles y responsabilidades asociadas de las partes involucradas en el SGSI, definidas en el apartado 3.5 Gestión de Roles y Responsabilidades. Durante el desarrollo de este proyecto se establecerán salvaguardas relativas al buen gobierno de la seguridad, y en dichos Comités se analizarán posibles mejoras en la organización, gestión de riesgos y la planificación de la seguridad. Adicional, como se ha comentado anteriormente, se presentarán los indicadores o mediciones de cumplimiento del SGSI descritos en el punto 3.3 Gestión de Indicadores.

COSTE:

El Responsable de la Seguridad de la Información será el encargado de convocar estos Comités, dirigirlos y presentarlos, siendo esta tarea una función asociada a su puesto, por tanto, el desarrollo de este proyecto no se considera un coste adicional.

PLANIFICACIÓN:

Cada 2 meses se celebrarán los Comités de seguimiento, retrasándose hasta 6 meses en casos excepcionales y justificados.

5.2.3 PRO-3: Plan de Externalización del Call Center

DESCRIPCIÓN:

Después de analizar si era viable que se implantasen todos los controles de seguridad que minimizasen el riesgo del servicio de call center, se ha visto que supondría un enorme coste para la organización. Por tanto, se ha tomado la decisión de que una empresa externa especializada en call center tome la gestión de dicho servicio, haciéndose cargo y comprometiéndose a asegurar dicho servicio mediante la firma de los correspondientes SLA (acuerdos de nivel de servicio) y NDA (acuerdos de confidencialidad).

Externalizar dicho servicio no solo permitirá ahorro de costes a la organización tales como mantenimiento y ampliación del edificio donde se encontraban que cada vez se iba quedando más pequeño, o el mantenimiento de todos los sistemas de información hardware y software adheridos al servicio, si no que se mejorará la calidad del servicio, el aseguramiento de su disponibilidad, la realización de copias de seguridad, formación especializada en dar el servicio, mejora en la gestión de la volumetría de llamadas, etc. todo ello dando como resultado un mejor servicio de atención al cliente y una mejor comercialización de productos.

Las salvaguardas que entran dentro de este proyecto de externalización del servicio deben tener en cuenta la relación con el proveedor externo, la implantación de acuerdos para intercambio de información y software, el acceso de externos a la información, y las relaciones con el personal externo subcontratado.

COSTE:

Después de haber hecho una media de la volumetría de llamadas entrantes y salientes de la organización, y haber estimado los recursos humanos necesarios, un posible proveedor de servicios externos de call center ha fijado el coste de prestarles el servicio de call center con tecnología voz IP en 60.000 €/mes.

PLANIFICACIÓN:

El posible proveedor externo del servicio de call center estima un plazo de traspaso completo del servicio de 4 meses. El gerente del área comercial se hará cargo del seguimiento del proyecto ya que de dicha área pende la supervisión y control del call

center, y reportará el seguimiento del proyecto a la Dirección, lo cual no quiere decir que empleados de otras áreas no apoyen con el traspaso de este servicio.

5.2.4 PRO-4: Plan de Bastionado de Servidores

DESCRIPCIÓN:

El proyecto va a consistir en poner mayor grado de seguridad a los sistemas que contienen información que se van a tratar, con el objetivo de impedir ataques o la modificación de la configuración base por parte de usuarios no autorizados, impidiendo que los usuarios saquen información de la organización de manera no autorizada, y minimizando los riesgos de que éstos se vean infectados por software malicioso manteniendo el software antivirus actualizado. Por tanto, se desplegará en todos los servidores que se encuentran en el CPD (servidor de negocio, de correo, de configuración y gestión de la seguridad, de RRHH, de DA…) directivas de seguridad atendiendo al servicio que prestan, con una configuración adecuada que mitigue o evite los riesgos sobre ellos.

COSTE:

Coste adicional (no se cuenta el sueldo asociado a los empleados que lo implanten) de 0 €. El despliegue e implantación de directivas las llevará a cabo el departamento de TI, en concreto el personal que gestiona el Directorio Activo, que serán los que desplieguen las directivas de seguridad acordadas en la guía de bastionado que se desarrolle y apruebe la Dirección.

PLANIFICACIÓN:

La elaboración de la guía de bastionado de servidores y la implantación de directivas se llevará a cabo en 2 meses.

5.2.5 PRO-5: Plan de Externalización del servicio de destrucción de la información

DESCRIPCIÓN:

Este proyecto se propone para la destrucción de manera segura de hardware (discos duros antiguos de ordenadores de sobremesa, disco duro de portátiles, servidores, USB u otros soportes físicos) y documentación que contienen información confidencial de la organización, pudiéndose proteger de fugas de información y del incumplimiento de la nueva ley de privacidad de los datos que ha entrado en vigor. Evidentemente, los activos que están bajo tratamiento por nivel alto o medio están dentro de este proyecto. Como se ha descubierto en el análisis diferencial, la organización no tiene ningún procedimiento de destrucción ni de documentos ni de destrucción física segura se soportes o discos duros obsoletos. Cuando se quiere destruir o eliminar información

de un dispositivo, se realiza un formateo normal de disco, corriendo el riesgo de que la información sea recuperable, y cuando se trata de información confidencial en papel, se guarda en un archivo o se rompe en pedazos.

Por tanto, por un lado, se ha decidido subcontratar el servicio de la destrucción de hardware obsoleto de manera puntual para que, cuando sea necesario, sean destruidos de manera segura. La empresa subcontratada debe cumplir con el protocolo de seguridad de la Cadena de Custodia hasta su destrucción física y proveer de un certificado de destrucción que confirme que el material ha sido destruido de forma segura.

Por otro lado, se ha decidido comprar dos trituradoras de papel para la destrucción de los documentos en papel.

COSTE:

El coste de la adquisición de las trituradoras es de 300€ cada una, suponiendo un total de 600€. Por otro lado, se ha contemplado para un futuro, la opción de contar con un servicio especializado de destrucción de soportes cuando sea necesario, que dependerá de los soportes que se quiera destruir.

PLANIFICACIÓN:

Duración de dos semanas para el análisis e implantación de la solución trituradora.

5.2.6 PRO-6: Plan de Revisiones Técnicas de Seguridad de la DMZ

DESCRIPCIÓN:

Este proyecto se pensó para evaluar la seguridad de la aplicación Web comercial y portal para contratar pólizas que tienen expuesta en la DMZ y mejorar su seguridad, pero se ha llegado a un acuerdo con la sede central en España para que el equipo especializado de Revisiones Técnicas que tienen allí, realicen una revisión técnica de seguridad de todos los sistemas de información que tienen publicados en su DMZ, tanto a nivel de aplicación como de infraestructura, lo cual les permitirá analizar las vulnerabilidades que tienen sus sistemas y establecer un plan de corrección de las mismas.

Para la realización de las revisiones técnicas de seguridad, el equipo establecido en la sede central corporativa, se basa en metodologías de reconocimiento internacional como son OWASP (*Open Web Application Security Project*) y OSSTMM (*Open Source Security Testing Methodology Manual*).

COSTE:

Coste de 0 €, ya que el test de intrusión lo realizará el personal de corporativo ubicado en España, a los que el departamento de IT les pasará el alcance a analizar.

PLANIFICACIÓN:

La duración del proyecto será aproximadamente de 2 meses, divida en lo siguiente:

- Primer mes: La primera mitad será para la planificación y preparación del alcance a analizar, y la segunda mitad de mes para la ejecución de pruebas.
- Segundo mes: Verificación de los resultados y generación del entregable con las vulnerabilidades descubiertas y las acciones correctivas.

Una vez realizado el test de intrusión, se debería proceder la resolución de las vulnerabilidades encontradas, cuyo encargo será asignado al departamento de TI, resolviendo las vulnerabilidades críticas y altas en un plazo de tres meses, y con un margen mayor para el resto de vulnerabilidades halladas.

5.2.7 PRO-7: Planes de Concienciación en Seguridad y Formación

DESCRIPCIÓN:

Durante el análisis diferencial, se ha detectado que varias de las amenazas con probabilidad alta de ocurrencia, van ligadas a los errores cometidos por los empleados de la organización. Por tanto, se quiere establecer por un lado, un plan de concienciación en seguridad y uso adecuado de herramientas y aplicaciones de la organización, y por otro lado, un plan de formación acorde al puesto de trabajo para el personal de la empresa, que vaya ligado a la seguridad de la información. Por tanto, los planes de formación se dividen en dos debido a si el personal que imparte la formación es interno o externo:

- Formación que impartirá personal interno: formación y concienciación en seguridad, consistente en superar un e-learning y asistir a una charla obligatoria explicando conceptos sobre seguridad (como tratar la información, qué hacer en caso de emergencia, etc.) y explicación de la Política de Seguridad de la Información para todos los empleados. Por otro lado, también se dará formación obligatoria de cómo usar adecuadamente el Sistemas de gestión de pólizas y otros trámites necesarios para negocio, y la Plataforma operativa de atención al cliente del CC (en carretera, viaje, sanitaria).

  La elaboración del e-learning será llevada a cabo por RRHH y la charla explicando conceptos de seguridad la llevará a cabo el Responsable de Seguridad de la Información. La explicación de uso adecuado del Sistemas de gestión de pólizas y otros trámites necesarios para negocio la llevará a cabo personal del área de finanzas. La explicación de uso adecuado de la Plataforma operativa de atención al cliente del CC la impartirá el área comercial.

- Formación que impartirá personal externo: formación especializada en seguridad de la información para cada una de las áreas (TI, Legal, marketing, etc.).

  También se incluirá formación externa especializada en SGSI para los responsables del SGSI.

COSTE:

El Departamento de Recursos Humanos, con la aprobación de la Dirección, será el encargado de elaborar el Plan completo de formación en seguridad de la información para todos los empleados. El coste principalmente vendrá asociado a la formación prestada por personal externo, a la que se destinará 60.000€/anuales.

PLANIFICACIÓN:

- Formación y concienciación en seguridad (Charla obliatoria + e-learning): 1 mes
- Formación obligatoria en uso de aplicaciones de la organización: 1 mes
- Formación especializada para los Responsables del SGSI: 1 mes
- Formación especializada sobre seguridad para cada área: 9 meses

5.2.8 PRO-8: Plan de mejora de la seguridad del CPD

DESCRIPCIÓN:

Durante el análisis diferencial, se han hallado varias deficiencias en cuanto a la seguridad del CPD, estando dentro de riesgos no asumibles varios activos asociados a él o que dependen de él, para su correcto funcionamiento. Por tanto, se proponen las siguientes sub-tareas enmarcadas en el citado plan de mejora para subsanar las deficiencias encontradas:

- Implantación de un sistema de autenticación de doble factor para la mejora del control de acceso basado en una tarjeta de coordenadas: A parte del identificador de usuario y contraseña que se debe introducir para acceder al CPD, se tiene que meter una clave sustraída de la tarjeta de coordenadas que pedirá el sistema si se quiere acceder al CPD. La entrega de esa tarjeta será suministrada después de haber sido aprobada por el Responsable de Seguridad. Además, este sistema permitirá registrar los accesos al CPD.

- Elaboración de un Plan de Recuperación ante Desastres (DRP): A pesar de que la organización ya cuenta con elementos identificados para hacer frente en caso de indisponibilidad de los sistemas del CPD o que evitan que ocurran ciertas amenazas, como puede ser los SAI, equipos de climatización, alarma y extinción de incendios, se quiere realizar y desarrollar un estudio más amplio y formal de Recuperación ante Desastres. Se llevará a cabo por parte de una consultora externa, que analizará todos los datos, hardware y software crítico de la organización, para que, en caso de desastre natural o humano, se puedan levantar los procesos y recuperar la información. Actualmente, se tiene que tener en cuenta que la organización solo envía respaldos a la nube de un proveedor de la información de interés primordial para negocio, relativa a clientes, pólizas y asistencias, pero no incluye el resto de información de la organización ni el software.

Adicional a esto, se deben seguir teniendo controladas las condiciones ambientales de temperatura y humedad de la sala con los sistemas de los que se disponen.

El principal responsable de supervisar este proyecto será el Responsable de Seguridad de la Información.

COSTE:

- Coste del sistema de autenticación de doble factor: 200 €. El coste va asociado principalmente a la instalación física del sistema donde los usuarios deban introducir los datos de autenticación.

- Presupuesto dedicado para el estudio de los procesos e infraestructura de TI para la elaboración del Plan de Recuperación ante Desastres: 40.000 €.

- Coste de la contratación de un servicio de copias de respaldo para realizar backups de toda la cantidad de información del CPD: 1.000 €/mes. Este precio puede variar si supera el rango de datos establecido en la tarifa. Por tanto, en principio, anualmente el coste total del servicio serían 12.000 €.

PLANIFICACIÓN:

- Instalación física del sistema de autenticación de doble factor: 1 día.

- Elaboración del Plan de Recuperación de Desastres por una consultora externa, que además lleva implícito el estudio y elección de del proveedor de copias de respaldo para hacer backups de toda la información del CPD: 3 meses.

5.2.9 PRO-9: Plan de Continuidad de Negocio

DESCRIPCIÓN:

El objetivo de este proyecto es establecer un Plan de Continuidad de Negocio para asegurar la continuidad de la seguridad de la información y la disponibilidad de todos los servicios, instalaciones, comunicaciones, servidores, aplicaciones y personal de la organización. El DRP explicado anteriormente forma parte de dicho Plan de Continuidad de Negocio, donde se deben acordar los debidos SLAs y el tiempo objetivo de recuperación y punto objetivo de recuperación de cada servicio a restaurar.

El principal responsable de supervisar este proyecto será el Responsable de Seguridad de la Información.

COSTE:

El presupuesto asignado para el desarrollo de este proyecto asciende a los 80.000 € y será llevado a cabo por una consultora externa.

PLANIFICACIÓN:

El Plan de Continuidad de Negocio se iniciará cuando finalice y apruebe el Plan de Recuperación de Desastres y durará otros 2 meses más.

5.3 PLANIFICACIÓN DEL PLAN DE MEJORAS

Se ha decidido elaborar un diagrama de Gantt para ver los diferentes proyectos en el transcurso de los meses. A cada proyecto se le ha asignado uno o varios recursos encargados de desplegar los proyectos de mejora para disminuir el riesgo de los activos a los que está expuesta la organización mediante dichos proyectos, y aparecen en el diagrama de Gantt. El significado de las siglas de los responsables que se han asignado a los proyectos en el diagrama de Gantt son los siguientes:

- RSI: Responsable de Seguridad de la Información
- DIR: Dirección
- EXSGSI: Consultora externa para la implementación del SGSI
- EXFOR: Empresas externas para dar formación
- EXCC: Empresa externa proveedora del servicio de call center
- EXCN: Empresa externa para la implantación de un Plan de Continuidad de Negocio
- EX2FAC: Empresa externa de instalación del doble factor de autenticación en el CPD
- TI: Área Técnica
- AI: Auditoría Interna
- RH: Área Recursos Humanos
- COR: Sede Corporativa
- OP: Área Operaciones
- CM: Área Comercial y Marketing
- LG: Área Legal
- FIN: Área Finanzas

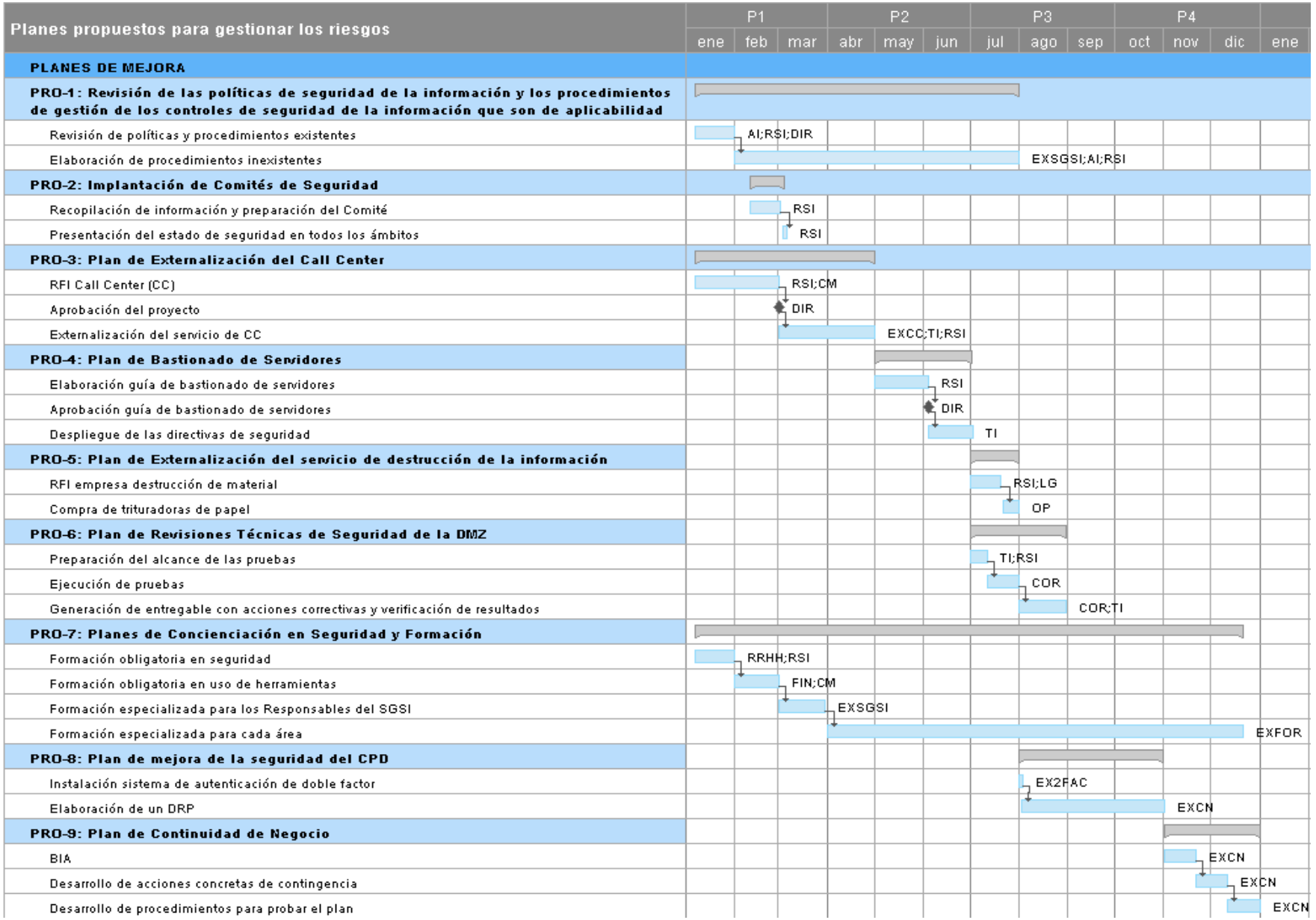

Fig. 7: Diagrama de Gantt de los proyectos

5.4 EVOLUCIÓN DE LOS RESULTADOS

A continuación, se presenta un diagrama de radar con la evolución de los diferentes dominios y su cumplimiento antes y después de la realización de los diferentes proyectos, pasando de un nivel inicial total de cumplimiento del 55% a un nivel final del 80% (por encima del nivel adecuado establecido por la organización):

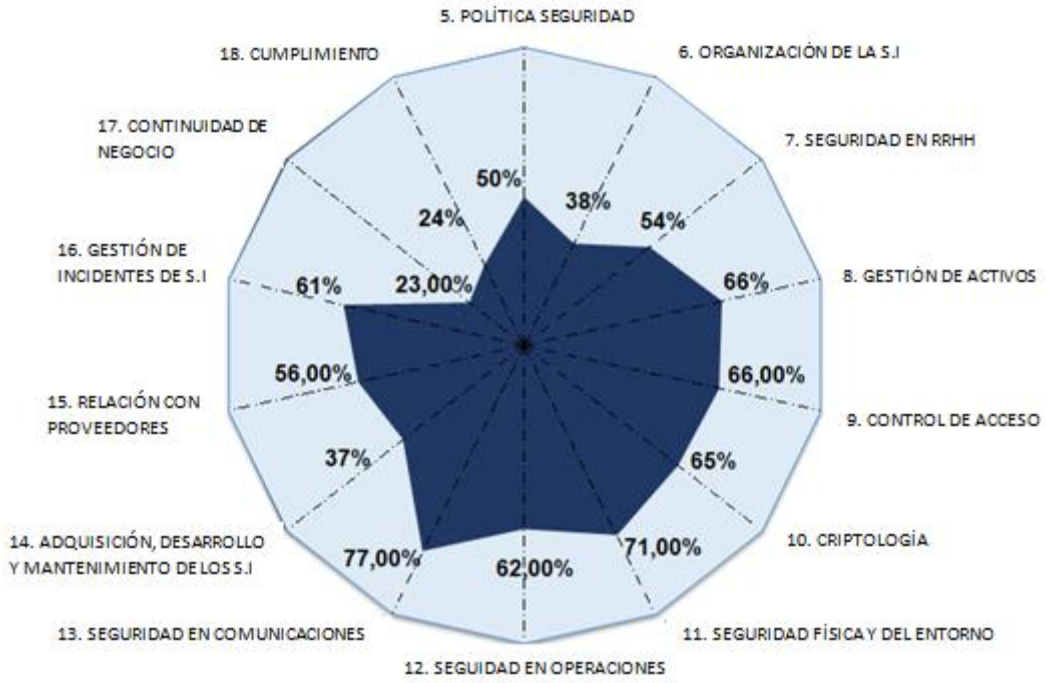

Fig. 5: Grado de adecuación actual de la organización a la norma de referencia ISO 27002

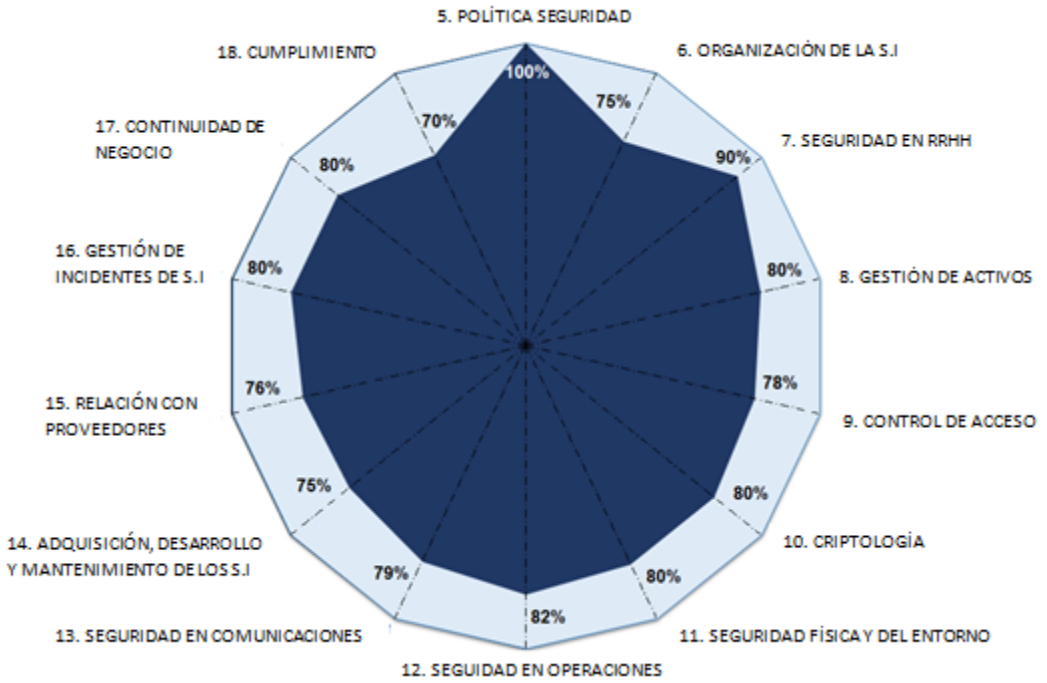

Fig. 8: Grado de adecuación a la ISO 27002 después de la implantación de los proyectos.

6. AUDITORÍA DE CUMPLIMIENTO

6.1 AUDITORÍA DE CUMPLIMIENTO DEL SGSI

Para evaluar el estado de implementación del Sistema de Gestión de Seguridad de la información y el nivel de avance en la implementación de los proyectos, la empresa se va a someter a la primera auditoría interna de cumplimiento del SGSI.

La auditoría se va a llevar a cabo 10 meses después de decidir implantar el SGSI y haber llevado a cabo los proyectos de mejora propuestos, escogidos para hacer frente a los principales riesgos identificados asociados a determinados activos importantes en la organización.

Después de finalizar la auditoría interna de cumplimiento, los resultados serán presentados a la Dirección cuando ésta lo requiera durante el proceso de revisión del SGSI descrito en el apartado 3.4 Procedimiento de Revisión por la Dirección, y el informe elaborado será divulgado a todas las partes interesadas.

Se anexa junto a este trabajo el informe de auditoría de cumplimiento con los hallazgos identificados en el documento "Informe de Auditoría Interna de Cumplimiento del SGSI".

6.2 EVALUACIÓN DE LA MADUREZ

Adicionalmente, la organización ha decidido proceder a evaluar el nivel de madurez de los requisitos que se requerían para la implantación de un SGSI, y el nivel de madurez de la seguridad de los controles aplicados, utilizando el Modelo de Madurez de la Capacidad (CMM) cuya tabla de niveles está definida en el apartado 3.6 Metodología de Análisis de Riesgos. También han evaluado el cumplimiento de las normas en base a la evaluación de la madurez de las mismas. Esta información también se tiene en cuenta durante la auditoría para evaluar el nivel de madurez existente en la organización respecto a las normas ISO 27001 e ISO 27002.

6.2.1 EVALUACIÓN DE LA MADUREZ DE LOS REQUERIMIENTOS DE LA ISO 27001

	CMM		
REQUISITOS ISO 27001	**NIVEL**	**EFECTIVIDAD**	**COMENTARIOS**
4. CONTEXTO DE LA ORGANIZACIÓN		**95%**	**Conforme**
4.1 Compresión de la organización y de su contexto	L4	95%	Gracias al estudio general de la organización para implantar un SGSI, ésta ha sido más conocedora de los riesgos a los que se enfrentan, sobre todo ahora que el negocio de la organización está empezando a crecer y el servicio de call center presentaba deficiencias. Han valorado la externalización de servicios y en un futuro no descartan tener externalizados otras partes de sus procesos operativos para alcanzar mejoras en los servicios.
4.2 Comprensión de las necesidades y expectativas de las partes interesadas	L4	95%	El análisis de riesgos ha proporcionado a la organización una visión más clara de sus necesidades. La Dirección espera que el SGSI les ayude a cumplir con los requisitos legales a los que se enfrentan, los requisitos de seguridad que sus clientes les exige, y esperan gestionar de manera adecuada la seguridad de la información de su organización, sobre todo en las áreas operativas como son las del call center y la comercial, con el apoyo de las áreas de legal, recursos humanos y TI.
4.3 Determinación del alcance del sistema de gestión de la seguridad de la información	L4	95%	Se ha determinado el alcance y los activos principales que entran dentro del SGSI, y será el que se tome como referencia para evaluar la mejora de su implementación.
4.4 Sistema de gestión de la seguridad de la información	L4	95%	Existe un SGSI implantado y se han llevado a cabo los principales proyectos de mejora propuestos. El SGSI se está evaluando actualmente.

5. LIDERAZGO		**97%**	**Conforme**
5.1 Liderazgo y compromiso	L4	95%	Se ha definido un procedimiento de Revisión por la Dirección y se han asignado los Roles y Responsabilidades.
5.2 Política	L5	100%	Ya se disponía de una Política de Seguridad de la Información que ha sido revisada y actualizada, además de establecerse un periodo de revisión de la misma durante la implantación del proyecto de mejora propuesto sobre este punto.
5.3 Roles, responsabilidades y autoridades en la organización	L4	95%	Se han asignado los roles y responsabilidades.
6. PLANIFICACIÓN		**95%**	**Conforme**
6.1 Acciones para tratar los riesgos y oportunidades	L4	95%	Se ha realizado una Declaración de Aplicabilidad, un Análisis de Riesgos y un Plan de tratamiento de riesgos o proyectos de mejora propuestos, para lograr la mejora de la seguridad de la información en la organización.
6.2 Objetivos de seguridad de la información y planificación para su consecución	L4	95%	Se ha establecido como objetivo implementar los requisitos y controles de la ISO/IEC 27001 y 27002, y también se han establecido procedimientos para la correcta implementación y consecución de las dos normas. En los Comités de Seguridad implantados se hará seguimiento del estado de las mismas y se mostrarán indicadores para ver el cumplimiento en seguridad de la organización.
7. SOPORTE		**93%**	**Conforme**
7.1 Recursos	L3	90%	La organización ha establecido claramente los recursos para la implementación inicial del SGSI, y no descarta destinar más recursos para conseguir una adecuada gestión de la seguridad.

7.2 Competencia	L3	90%	Las competencias necesarias de las personas se evaluarán mejor con la implantación del SGSI que establece mediciones de cumplimiento y evolución, y observa las mejoras conseguidas.
7.3 Concienciación	L4	95%	Se ha propuesto un proyecto de concienciación y formación en materia de seguridad de la información durante la implantación del SGSI que ha hecho que la organización mejore en este aspecto.
7.4 Comunicación	L4	95%	El establecimiento de responsabilidades y procedimientos ha hecho que las comunicaciones pertinentes sobre el sistema de gestión de la seguridad de la información mejoren.
7.5 Información documentada	L4	95%	Durante la implantación del SGSI, se ha creado un sistema de gestión documental basado en la norma ISO 27001, y se ha establecido un procedimiento de revisión y control de cambios del mismo.
8. OPERACIÓN		**92%**	**Conforme**
8.1 Planificación y control operacional	L4	95%	Durante la implantación del SGSI, la organización ha planificado los proyectos de mejora principales propuestos y las revisiones de sus procesos.
8.2 Apreciación de los riesgos de seguridad de la información	L3	90%	Para la implantación de este SGSI, se ha hecho necesario que la organización sepa los riesgos de seguridad de la información a los que se enfrenta, y se ha realizado una evaluación de los mismos.
8.3 Tratamiento de los riesgos de seguridad de la información	L3	90%	Para la implantación de este SGSI, se ha hecho necesario que la organización sepa los riesgos de seguridad de la información a los que se enfrenta, y se ha realizado un plan de tratamiento de los mismos.

9. EVALUACIÓN DEL DESEMPEÑO		**90%**	**Conforme**
9.1 Seguimiento, medición, análisis y evaluación	L3	90%	Con la realización de esta auditoría de cumplimiento del SGSI, se determina que la organización si está evaluando el desempeño del SGSI implantado y descrito en este Plan Director de Seguridad.
9.2 Auditoría interna	L3	90%	La implementación del SGSI ha dado pie a la realización periódica de auditorías internas para ver el cumplimiento de los aspectos en materia de seguridad de la información.
9.3 Revisión por la dirección	L3	90%	Durante la implantación del SGSI, se ha definido un procedimiento de revisión del SGSI por parte de la Dirección.
10. MEJORA		**50%**	**No conformidad menor**
10.1 No conformidad y acciones correctivas	L2	50%	Aún no existe documentación con no conformidades u observaciones por ser ésta la primera auditoría de cumplimiento y evaluación de madurez por la que pasa el SGSI, pero la organización tiene conciencia de la mejora continua que implica tener un SGSI implantado, y sí que han ido realizando acciones correctivas.
10.2 Mejora continua	L2	50%	Aún no existe documentación con no conformidades u observaciones por ser ésta la primera auditoría de cumplimiento y evaluación de madurez por la que pasa el SGSI, pero la organización tiene conciencia de la mejora continua que implica tener un SGSI implantado, y sí que han ido realizando acciones correctivas.

A continuación, se muestra el gráfico con los porcentajes de los niveles de madurez de los requisitos de implementación del SGSI de la organización:

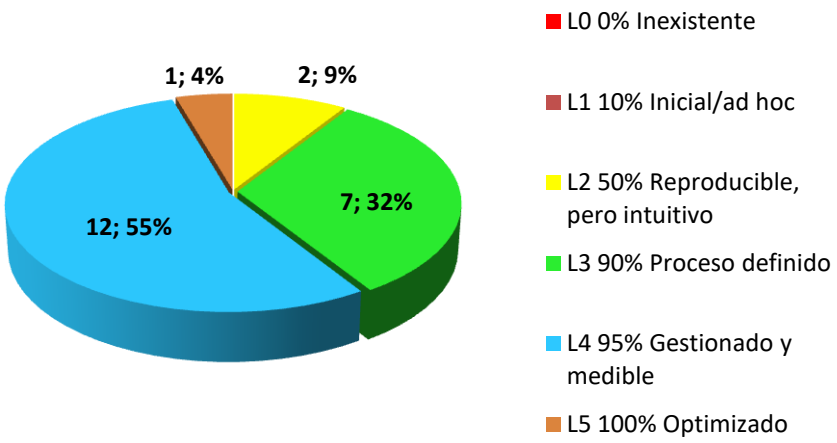

Fig. 9: Niveles de madurez de los requisitos de implementación del SGSI

6.2.2 EVALUACIÓN DE LA MADUREZ DE LOS CONTROLES DE LA ISO 27002

	CMM		
CONTROLES ISO 27002	**NIVEL**	**EFECTIVIDAD**	**COMENTARIOS**
5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN		**95%**	**Conforme**
5.1.1 Políticas para la seguridad de la información	L4	95%	La Política de Seguridad de la Información está documentada, publicada y comunicada a todos los empleados. Además todos los empleados han hecho un e-learning donde también se da a conocer la Política de Seguridad de la Información.
5.1.2 Revisión de las políticas para la seguridad de la información	L4	95%	Queda establecida la periodicidad de la revisión de las políticas y procedimientos de seguridad de la información y los responsables de revisar y mantener dichos documentos. Durante el transcurso de la implantación del SGSI se ha realizado la primera revisión.
6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		**84%**	**Observación**
6.1.1 Roles y responsabilidades en seguridad de la información	L4	95%	Se han definido los responsables y sus responsabilidades relativas a seguridad de la información de manera formal durante la implantación del SGSI, y se están llevando a cabo cada dos meses Comités de Seguridad para dar seguimiento a las acciones e indicadores principales de seguridad.
6.1.2 Segregación de tareas	L3	90%	Se han asignado adecuadamente las responsabilidades y tareas de cara a la implantación del SGSI.
6.1.3 Contacto con las autoridades	L3	90%	Se ha revisado y ampliado el listín telefónico para hacer uso de él en caso de emergencias. Éste ha sido distribuido y publicado en la intranet para que todos los empleados lo conozcan.

6.1.4 Contacto con grupos de interés especial	L3	90%	El Responsable de Seguridad de la Información está informado de las publicaciones y boletines del Equipo Nacional de Respuesta de Emergencias Informáticas (CERT) del país, y asistirá anualmente a un congreso nacional sobre Ciberseguridad celebrado en su país.
6.1.5 Seguridad de la información en la gestión de proyectos	L3	90%	Se ha definido que el Responsable de Seguridad de la Información sea el responsable de comunicar a corporativo todos los nuevos proyectos que surgen en la organización para que sean revisados desde el punto de vista de seguridad junto con el apoyo de él mismo. Se pasa un cuestionario con preguntas relativas a la seguridad en el proyecto y se contesta con ayuda del RSI. Después se genera un documento con recomendaciones previo a la puesta en marcha del proyecto. Hasta el momento se ha registrado el proyecto de externalización del call center.
6.2.1 Política de dispositivos móviles	L2	50%	Se ha desarrollado un procedimiento de uso correcto de dispositivos móviles, pero aún falta por implantar las medidas necesarias en los portátiles para protegerlos, como son el cifrado y la realización de copias de seguridad de éstos. Por tanto la responsabilidad de que no sufra ningún incidente queda a cargo del empleado.
6.2.2 Teletrabajo	N/A		La Declaración de Aplicabilidad expone que dicho control no aplica hasta el momento.
7. SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS		**92%**	**Conforme**
7.1.1 Investigación de antecedentes	L3	90%	El área de RRHH ha definido un procedimiento donde hace referencia a comprobar la veracidad de los datos previa a la contratación del empleado.
7.1.2 Términos y condiciones del empleo	L4	95%	Desde el inicio de la compañía, todos los empleados firman unos términos y condiciones de empleo, entre ellos la clausula de confidencialidad para proteger los datos de la organización y los términos que le aplican por el puesto que van a tener relativos a la seguridad de la información.
7.2.1 Responsabilidades de gestión	L3	90%	La Dirección ha difundido a todos los empleados la política de seguridad de la información y ha dado a conocer los procedimientos de seguridad de la información para que entiendan y cumplan la normativa establecida por la organización en esta materia.

7.2.2 Concienciación, educación y capacitación en seguridad de la información	L4	95%	El área de RRHH ha definido un Plan de Concienciación en Seguridad de la información y formación específica, y está llevando un seguimiento sobre el indicador de participación a las formaciones.
7.2.3 Proceso disciplinario	L3	90%	El área de RRHH ha definido y publicado un procedimiento.
7.3.1 Responsabilidades ante la finalización o cambio	L3	90%	El área de RRHH ha definido y publicado un procedimiento.
8. GESTIÓN DE ACTIVOS		**92%**	**Conforme**
8.1.1 Inventario de activos	L4	95%	Se ha establecido el seguimiento de los indicadores principales de seguridad que proporciona la herramienta de gestión de inventario de activos en los Comités de Seguridad para darles seguimiento y alcanzar una mejora continua mediante la realización de acciones correctivas.
8.1.2 Propiedad de los activos	L4	95%	Quedan definidos y documentados los propietarios de los activos que entran dentro del alcance del SGSI y la formación específica para cada uno de ellos. Anualmente se revisarán los propietarios por si se ha producido algún cambio o baja del personal.
8.1.3 Uso aceptable de los activos	L3	90%	Queda publicado en la Intranet el procedimiento de uso aceptable de los activos junto con el resto de procedimientos de la organización y la Política de Seguridad de la Información para el conocimiento de todo el personal de la organización.
8.1.4 Devolución de activos	L3	90%	Queda publicado en la Intranet el procedimiento de uso aceptable de los activos junto con el resto de procedimientos de la organización y la Política de Seguridad de la Información para el conocimiento de todo el personal de la organización.

8.2.1 Clasificación de la información	L3	90%	Queda publicado en la Intranet el procedimiento de uso aceptable de los activos junto con el resto de procedimientos de la organización y la Política de Seguridad de la Información para el conocimiento de todo el personal de la organización.
8.2.2 Etiquetado de la información	L3	90%	Queda publicado en la Intranet el procedimiento de uso aceptable de los activos junto con el resto de procedimientos de la organización y la Política de Seguridad de la Información para el conocimiento de todo el personal de la organización.
8.2.3 Manipulado de la información	L3	90%	Queda publicado en la Intranet el procedimiento de uso aceptable de los activos junto con el resto de procedimientos de la organización y la Política de Seguridad de la Información para el conocimiento de todo el personal de la organización.
8.3.1 Gestión de soportes extraíbles	L3	90%	Queda publicado en la Intranet el procedimiento de uso aceptable de los activos junto con el resto de procedimientos de la organización y la Política de Seguridad de la Información para el conocimiento de todo el personal de la organización.
8.3.2 Eliminación de soportes	L4	95%	Queda publicado en la Intranet el procedimiento de uso aceptable de los activos junto con el resto de procedimientos de la organización y la Política de Seguridad de la Información para el conocimiento de todo el personal de la organización. Se ha contratado una empresa de eliminación de material de manera segura, la cual emite un certificado de destrucción de material.
8.3.3 Soportes físicos en tránsito	N/A		
9. CONTROL DE ACCESO		**91%**	**Conforme**
9.1.1 Política de control de acceso	L3	90%	La política de control de acceso se ha divulgado a todos los empleados y se ha publicado en la Intranet.

9.1.2 Acceso a las redes y a los servicios de red	L3	90%	El procedimiento está implantado por el departamento de TI, dando determinados accesos al usuario dependiendo del recurso al que quieran acceder y estén autorizados para ello. Se tiene implantados controles y herramientas para controlar los accesos a la red y anomalías en la misma.
9.2.1 Registro y baja de usuarios	L4	95%	Procedimiento implantado por el departamento de TI, revisado por el RSI, y quedan establecidos los indicadores para ver si el proceso de registro y de baja en los sistemas se está llevando a cabo correctamente. También se ha establecido un indicador sobre la inactividad de usuarios para proceder a su bloqueo o darles de baja en caso de no uso.
9.2.2 Provisión de acceso de usuario	L3	90%	Está establecido un proceso de asignación de permisos de acceso según el rol y la necesidad de cada uno y la revisión periódica de dichos accesos junto con el propietario del sistema de información.
9.2.3 Gestión de privilegios de acceso	L4	95%	El departamento de TI y los responsables de autorizar los privilegios de acceso han elaborado un procedimiento para gestionarlos, registrándose todas las peticiones que llegan a los responsables o al departamento de TI, por tanto se pueden establecer indicadores de seguimiento.
9.2.4 Gestión de la información secreta de autenticación de los usuarios	L3	90%	Se ha mejorado el procedimiento de asignación de contraseñas y se han dotado de controles para el bloqueo automático del identificador de usuario y su inhabilitación temporal, con objeto de proteger a los sistemas frente a ataques por fuerza bruta, en los siguientes casos: por el número de intentos de acceso incorrectos y la por inactividad del usuario en el sistema. Además, se ha desarrollado un procedimiento de identificación y autenticación de usuarios y se ha divulgado y publicado para todo el personal.
9.2.5 Revisión de los derechos de acceso de usuario	L3	90%	Queda implantada la revisión periódica de accesos a los sistemas de información junto con el propietario de dicho sistema.
9.2.6 Retirada o reasignación de los	L3	90%	Queda implantada la revisión periódica de accesos a los sistemas de información junto con el propietario de dicho sistema.

derechos de acceso			
9.3.1 Uso de la información secreta de autenticación	L3	90%	Queda definido el dentro del procedimiento de control de accesos el uso de las contraseñas y está publicado en la intranet para todos los empleados.
9.4.1 Restricción del acceso a la información	L3	90%	Queda establecido un proceso de asignación de permisos de acceso según el rol y la necesidad de cada uno y la revisión periódica de dichos accesos junto con el propietario del sistema de información.
9.4.2 Procedimientos seguros de inicio de sesión	L3	90%	Se ha dado formación a personal del área de TI.
9.4.3 Sistemas de gestión de contraseñas	L3	90%	Se ha establecido un procedimiento para la gestión adecuada de contraseñas, que también muestran unos requisitos de cambio de contraseña y formato según sean usuarios normales o administradores.
9.4.4 Uso de utilidades con privilegios del sistema	L3	90%	Se ha dado formación a personal del área de TI.
9.4.5 Control de acceso al código fuente de los programas	L3	90%	Se ha desarrollado un procedimiento para el control de acceso al código fuente y se ha divulgado al área de TI.
10. CRIPTOGRAFÍA		**70%**	**Observación**
10.1.1 Política de uso de los controles criptográficos	L2	50%	Aún no están documentados y comunicados los procesos de manera formal.
10.1.2 Gestión de claves	L3	90%	Se ha establecido un procedimiento y se ha dado formación al personal del área de TI que gestiona las claves.

11. SEGURIDAD FÍSICA Y DEL ENTORNO		**93%**	**Conforme**
11.1.1 Perímetro de seguridad física	L4	95%	Se han revisado y actualizado los procedimientos de control de acceso al recinto, instalaciones, etc., mejorando el control de acceso al CPD con la implantación de un sistema de autenticación de doble factor. Quedan registrados todos los accesos al recinto automáticamente, y también se dispone de seguridad privada.
11.1.2 Controles físicos de entrada	L4	95%	Se han revisado y actualizado los procedimientos de control de acceso al recinto, instalaciones, etc., mejorando el control de acceso al CPD con la implantación de un sistema de autenticación de doble factor. El sistema nuevo permite controlar y registrar los accesos al CPD, igual que se permiten registrar los accesos y salidas del recinto con la herramienta instalada que lee las tarjetas de los empleados.
11.1.3 Seguridad de oficinas, despachos y recursos	L3	90%	Se han revisado y actualizado los procedimientos de control de acceso a las oficinas y recursos, y se obliga al personal a tener la tarjeta identificativa visible, y si no es empleado se exige una autorización en caso de ser necesario el acceso.
11.1.4 Protección contra las amenazas externas y ambientales	L4	95%	Las instalaciones cuentan con las protecciones contra incendios adecuadas, y se ha actualizado el procedimiento de revisión de los sistemas de protección. Se han revisado los procedimientos en caso de emergencia, y se imparten formaciones sobre emergencias en el e-learning y la charla presencial. El RSI ha implantado la realización de un simulacro anualmente y se realiza un informe donde se muestran los obstáculos encontrados y posibles mejoras a la hora de evacuar los edificios.
11.1.5 El trabajo en áreas seguras	L3	90%	Se ha mejorado el acceso a áreas seguras como puede ser al CPD, y se ha implantado un procedimiento que autorice la entrada a áreas seguras por parte del RSI.
11.1.6 Áreas de carga y descarga	L3	90%	Se han revisado los procedimientos llevados a cabo hasta el momento, donde se establecen unas zonas determinadas de carga y descarga sin información accesible, y se añade la necesidad de revisar la carga previamente a la entrada al edificio.

11.2.1 Emplazamiento y protección de equipos	L4	95%	La entrada al CPD está restringida y se le ha proporcionado mayor seguridad a la hora de acceder a él, además de tener controladas las condiciones ambientales de temperatura y humedad. Los equipos de los empleados del Edificio 1 cuentan con un filtro de privacidad para la pantalla.
11.2.2 Instalaciones de suministro	L3	90%	Se han revisado las instalaciones de suministro, estableciendo un periodo de revisión. Ambos edificios están conectados a grupos electrógenos que alimentan a los sistemas de energía ininterrumpida que serán usados en caso de apagones o si se produce algún incidente eléctrico.
11.2.3 Seguridad del cableado	L4	95%	El cableado de los edificios no es visible al público y el cableado del CPD está mejor protegido contra manipulaciones no autorizadas por mejorar el acceso a la sala.
11.2.4 Mantenimiento de los equipos	L3	90%	Todos los sistemas críticos que no se han externalizado, tienen contratado mantenimiento con los proveedores del producto.
11.2.5 Retirada de materiales propiedad de la empresa	L4	95%	Se ha revisado y divulgado el procedimiento de salida de materiales a las personas afectadas. Se registra la salida de equipos, soportes, etc. que es necesario que salgan de las instalaciones.
11.2.6 Seguridad de los equipos fuera de las instalaciones	L3	90%	Se ha dado formación a todo el personal para saber cómo mantener protegidos sus documentos y equipos portátiles fuera de las instalaciones. Se divulgan unas guía de seguridad con consejos de cómo mantener seguros los documentos y equipos de la organización fuera de las instalaciones.
11.2.7 Reutilización o eliminación segura de equipos	L4	95%	Se ha externalizado el servicio de eliminación segura de equipos, quien lleva un registro de los materiales y destruidos y están certificados en destrucción segura de materiales.
11.2.8 Equipo de usuarios desatendido	L3	90%	Se ha dado formación a todos los empleados. Si se detecta inactividad en las aplicaciones principales o en el propio equipo, se pide de nuevo la contraseña al usuario en la aplicación o se bloquea la pantalla del ordenador.

11.2.9 Política de puesto de trabajo despejado y pantalla limpia	L4	95%	Se ha dado formación a todos los empleados para que la documentación que no estén usando no la dejen visible o la que no sea necesaria la destruyan en las nuevas trituradoras. El edificio 1 dispone de cajoneras. Los empleados del call center no tenían, pero se ha externalizado el servicio. Se ha procedido a etiquetar las cajoneras y estantes existentes para tenerlo inventariado y controlado.
12. SEGURIDAD DE LAS OPERACIONES		**93%**	**Conforme**
12.1.1 Documentación de procedimientos de la operación	L3	90%	Se han desarrollado, establecido y divulgado a las personas necesarias todos los procedimientos de operación de los sistemas que entran dentro del alcance del SGSI.
12.1.2 Gestión de cambios	L4	95%	Se han establecido los procedimientos para la gestión de cambios de los servicios y sistemas que entran dentro del alcance del SGSI, llevando un registro de cambios de cada uno de los sistemas.
12.1.3 Gestión de capacidades	L3	90%	Con la externalización de los servicios de call center y de copias de respaldo del CPD se va a controlar y gestionar mejor las capacidades actuales y futuras necesarias mediante acuerdos con el proveedor.
12.1.4 Separación de los recursos de desarrollo, prueba y operación	L4	95%	Los entornos de desarrollo, pruebas y producción están debidamente separados. Se ha revisado el procedimiento de desarrollo de software y se ha impartido formación a los desarrolladores del departamento de TI para que integren la seguridad de la información en el ciclo de vida de desarrollo.
12.2.1 Controles contra el código malicioso	L4	95%	Se han establecido indicadores para medir la protección y seguir el estado de seguridad de la organización y reportarlo en los Comités (indicadores de nivel de instalación del AV, de actualización de firmas, de despliegue de parcheado, etc.).
12.3.1 Copias de seguridad de la información	L4	95%	El servicio de externalización de copias sigue el procedimiento que se ha acordado con la Dirección para las copias de seguridad de la información del CPD que entra dentro del alcance del SGSI.

12.4.1 Registro de eventos	L3	90%	Se ha desarrollado un procedimiento de gestión de eventos donde se obliga a tener un registro de los eventos producidos en los sistemas que entran dentro del alcance del SGSI.
12.4.2 Protección de la información de registro	L4	95%	Está establecido que solo determinadas personas con el rol de administrador pueden acceder a la información de registro. Se ha establecido un procedimiento para la gestión de registros.
12.4.3 Registros de administración y operación	L4	95%	Se han habilitado los registros para las auditorías en todos los sistemas que entran dentro del alcance del SGSI independientemente del usuario que acceda, por tanto quedan registradas también las acciones de los administradores.
12.4.4 Sincronización del reloj	L3	90%	Para mantener la consistencia de los registros de eventos entre sistemas, los relojes de dichos sistemas han sido sincronizados entre sí mediante el uso de una fuente de tiempo externa fiable.
12.5.1 Instalación del software en explotación	L3	90%	Se han revisado y actualizado los procedimientos existentes y se ha formado al personal de TI.
12.6.1 Gestión de las vulnerabilidades técnicas	L4	95%	Se analizan el nivel de parcheado de los sistemas gracias a la herramienta de gestión de inventario, sabiendo así el nivel de vulnerabilidad con respecto al parcheado. Se ha realizado un test de intrusión donde se han detectado un cierto número de vulnerabilidades clasificadas según su nivel de criticidad. Se dará seguimiento de dichas vulnerabilidades descubiertas y del nivel de vulnerabilidad respecto a parcheado en los Comités de Seguridad.
12.6.2 Restricción en la instalación de software	L3	90%	Se han revisado y actualizado los procedimientos existentes y se ha formado al personal de TI.
12.7.1 Controles de auditoría de sistemas de información	L3	90%	Se ha realizado un test de intrusión sin afectar a la operativa diaria.
13. SEGURIDAD DE LAS COMUNICACIONES		**93%**	**Conforme**

13.1.1 Controles de red	L4	95%	Se realizan mediciones tanto de rendimiento como de seguridad en la red que luego se presentan en los Comités de Seguridad.
13.1.2 Seguridad de los servicios de red	L4	95%	Se han elaborado procedimientos de configuración de los elementos de seguridad de la red y se han divulgado por el departamento de TI. Se han establecido indicadores para ver el nivel de bastionado de los servidores.
13.1.3 Segregación en redes	L4	95%	Las redes se encuentran segregadas y se ha revisado por parte del departamento de TI dicha segregación en grupos de usuarios, sistemas o servicios para ver si todos los objetos están bien ubicados.
13.2.1 Políticas y procedimientos de intercambio de información	L3	90%	Están establecidos procedimientos con el banco, clientes y proveedores.
13.2.2 Acuerdos de intercambio de información	L3	90%	Están establecidos procedimientos con el banco, clientes y proveedores.
13.2.3 Mensajería electrónica	L3	90%	Queda publicado en la intranet el procedimiento de mensajería electrónica para que lo conozca y aplique todo el personal.
13.2.4 Acuerdos de confidencialidad o no revelación	L4	95%	Queda establecido que durante el proceso de contratación, empleado y proveedores externos firmen un acuerdo de confidencialidad para asegurar los datos que manejen de la organización.
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS S. DE INFORMACIÓN		**82%**	**Observación**

14.1.1 Análisis de requisitos y especificaciones de seguridad de la información	L4	95%	Se ha establecido un procedimiento para incluir la seguridad desde el inicio de los proyectos o nuevos sistemas de información. En las charlas de formación se ha trasladado que cuando se quiera llevar a cabo una nueva iniciativa, ésta debe ser consultada con el Responsable de Seguridad de la Información y lo trasladará a la sede central de corporativo para que el equipo de nuevas iniciativas de allí establezcan unos requisitos de seguridad, los cuales trasladarán en un informe, y se dará seguimiento de su implantación.
14.1.2 Asegurar los servicios de aplicaciones en redes públicas	L4	95%	Se ha realizado un test de intrusión para ver las debilidades que podrían tener las aplicaciones y sistemas que prestan servicios y poder proceder a su resolución.
14.1.3 Protección de las transacciones de servicios de aplicaciones	L3	90%	Las transacciones de datos entre servicios, tanto de las aplicaciones que se gestionan internamente como de la plataforma del servicio de call center, que pasa a ser gestionado por un externo, se producen mediante comunicaciones cifradas. Se ha realizado un test de intrusión para ver las debilidades que podrían tener las aplicaciones y sistemas y proceder a su resolución.
14.2.1 Política de desarrollo seguro	L3	90%	Se ha establecido un procedimiento de desarrollo seguro, se ha publicado en la intranet y en la formación específica se ha recordado al personal de TI.
14.2.2 Procedimiento de control de cambios en sistemas	L3	90%	Se ha establecido un procedimiento de control de cambios, se ha publicado en la intranet y en la formación específica se ha recordado al personal de TI.
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	L3	90%	Se ha establecido y mejorado el procedimiento existente y se ha formado al personal de TI.
14.2.4 Restricciones a los cambios en los paquetes de software	L3	90%	Se ha establecido y mejorado el procedimiento existente y se ha formado al personal de TI.

14.2.5 Principios de ingeniería de sistemas seguros	L2	50%	Se deben definir unas técnicas o requerimientos de ingeniería de seguridad mínimos para aplicarse a los sistemas de información de la organización, tanto internos como externos, yendo alineados con los procedimientos de seguridad ya definidos.
14.2.6 Entorno de desarrollo seguro	L3	90%	Existe un entorno de desarrollo seguro, separado del entorno de pruebas y de producción.
14.2.7 Externalización del desarrollo de software	L4	95%	Se ha mejorado el procedimiento existente y se le ha dado a conocer al personal de TI.
14.2.8 Pruebas funcionales de seguridad de sistemas	L3	90%	Se ha establecido y mejorado el procedimiento existente y se ha formado al personal de TI.
14.2.9 Pruebas de aceptación de sistemas	L3	90%	Se ha establecido y mejorado el procedimiento existente y se ha formado al personal de TI.
14.3.1 Protección de los datos de prueba	L2	50%	No existe un procedimiento determinado para los datos de pruebas, pero se controla el acceso al entorno de pruebas.
15. RELACIÓN CON PROVEEDORES		**74%**	**Observación**
15.1.1 Política de seguridad de la información en las relaciones con los proveedores	L3	90%	Están establecidos unos requerimientos de seguridad en los contratos con los proveedores.
15.1.2 Requisitos de seguridad en contratos con terceros	L3	90%	Están establecidos unos requerimientos de seguridad en los contratos con los proveedores.

15.1.3 Cadena de suministros de tecnología de la información y de las comunicaciones	L3	90%	Se ha revisado el procedimiento que incluye la cumplimentación de un cuestionario por parte del proveedor para ver si el proveedor cumple con los requisitos mínimos de seguridad de la información para poder prestar el servicio.
15.2.1 Control y revisión de la provisión de servicios del proveedor	L1	10%	No existen procedimientos de revisiones o auditorías sobre la provisión de servicios del proveedor del call center, el de copias de respaldo o el de destrucción de material.
15.2.2 Gestión de cambios en la provisión del servicio del proveedor	L3	90%	Se ha establecido un procedimiento de revisión de los cambios que pueden surgir durante la provisión de un servicio, donde existe una comunicación bilateral de los cambios o mejoras realizadas por la organización y por parte del proveedor.
16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN		**92%**	**Conforme**
16.1.1 Responsabilidades y procedimientos	L4	95%	Se han revisado los procedimientos para la gestión de eventos e incidentes y se ha formado al personal de TI y al Responsable de Seguridad de la Información en el uso de herramientas para la gestión de eventos. Se ha divulgado que todos los incidentes de seguridad deben ser comunicados al RSI y se ha elaborado un registro de incidentes para guardar su evaluación y tratamiento.
16.1.2 Notificación de los eventos de seguridad de la información	L3	90%	Se han revisado los procedimientos de notificación de eventos y se ha divulgado en las charlas de formación que todos los incidentes de seguridad deben ser comunicados al RSI. El RSI también comunicará aquellos incidentes de seguridad de nivel alto o grave a la sede central para que lo evalúen y le den las recomendaciones oportunas.

16.1.3 Notificación de puntos débiles de la seguridad	L3	90%	Se han revisado los procedimientos de notificación de eventos y se ha divulgado en las charlas de formación que todos los incidentes de seguridad deben ser comunicados al RSI. El RSI también comunicará aquellos incidentes de seguridad de nivel alto o grave a la sede central para que lo evalúen y le den las recomendaciones oportunas.
16.1.4 Evaluación y decisión sobre los eventos de seguridad de información	L3	90%	Se han revisado los procedimientos de gestión de eventos y se ha elaborado un registro de incidentes para guardar su evaluación y tratamiento.
16.1.5 Respuesta a incidentes de seguridad de la información	L3	90%	Se han revisado los procedimientos de gestión de eventos y se ha elaborado un registro de incidentes para guardar su evaluación y tratamiento.
16.1.6 Aprendizaje de los incidentes de seguridad de la información	L4	95%	Se han revisado los procedimientos de gestión de eventos y se ha elaborado un registro de incidentes para guardar su evaluación y tratamiento.
16.1.7 Recopilación de evidencias	L4	95%	Se han revisado los procedimientos y se ha elaborado un registro de incidentes donde se podrán guardar adjuntos con evidencias, documentación, etc.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO		**50%**	**No conformidad menor**

17.1.1 Planificación de la continuidad de la seguridad de la información	L2	50%	El Plan de Continuidad de Negocio está pendiente finalizarlo y se está teniendo en cuenta la disponibilidad de todos los servicios, instalaciones, comunicaciones, servidores, aplicaciones y personal de la organización, en caso de un desastre o crisis. Durante la elaboración del BIA para la gestión de la continuidad y el DRP se han considerado los requisitos de seguridad de la información que son aplicables en situaciones adversas.
17.1.2 Implementar la continuidad de la seguridad de la información	L2	50%	Se está desarrollando un Plan de Continuidad de Negocio que incluye todos los activos afectados y los riesgos identificados durante el análisis. Se va a dar formación a determinado personal el cual también está participando en la elaboración del mismo junto con la consultora externa.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	L2	50%	La organización va a establecer un plan de pruebas de continuidad de negocio para asegurar que la organización puede recuperarse ante un desastre, y también incluirá pruebas del DRP para medir los tiempos mínimos de recuperación de la infraestructura y los servicios críticos, y se comprobará cada cierto tiempo que se pueden restablecer las copias.
17.2.1 Disponibilidad de los recursos de tratamiento de la información	L2	50%	Se está desarrollando un Plan de Continuidad de Negocio que garantice la disponibilidad de los sistemas de información que entran dentro del alcance del SGSI en caso de desastre o crisis.
18. CUMPLIMIENTO		**81%**	**Observación**
18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales	L3	90%	Se ha dado formación al departamento de Legal y al Responsable de Seguridad de la Información para establecer procedimientos que cumplan con la legislación vigente.

18.1.2 Derechos de propiedad intelectual (DPI)	L3	90%	Se ha establecido un procedimiento para la gestión de las licencias.
18.1.3 Protección de los registros de la organización	L3	90%	Se ha establecido un procedimiento de revisión periódico de los principales registros.
18.1.4 Protección y privacidad de la información de carácter personal	L3	90%	Se han desarrollado procedimientos para asegurar la protección de los datos. Se evaluará la eficacia de las medidas mediante auditorías, aún no se ha hecho ninguna.
18.1.5 Regulación de los controles criptográficos	L1	10%	La organización no contempla procedimientos o acciones respecto a este control.
18.2.1 Revisión independiente de la seguridad de la información	L3	90%	Esta es la primera auditoría de cumplimiento a la que se somete la organización. Se han establecido procedimientos y un plan de auditoría.
18.2.2 Cumplimiento de las políticas y normas de seguridad	L3	90%	Esta es la primera auditoría de cumplimiento a la que se somete la organización. Se han establecido procedimientos y un plan de auditoría.
18.2.3 Comprobación del cumplimiento técnico	L4	95%	Se ha realizado un test de intrusión para ver las debilidades que podrían tener los sistemas de información que prestan servicios, hacer seguimiento de las mismas y poder proceder a su resolución.

A continuación, se muestra el gráfico con los porcentajes de los niveles de madurez de los controles de seguridad implantados en la organización:

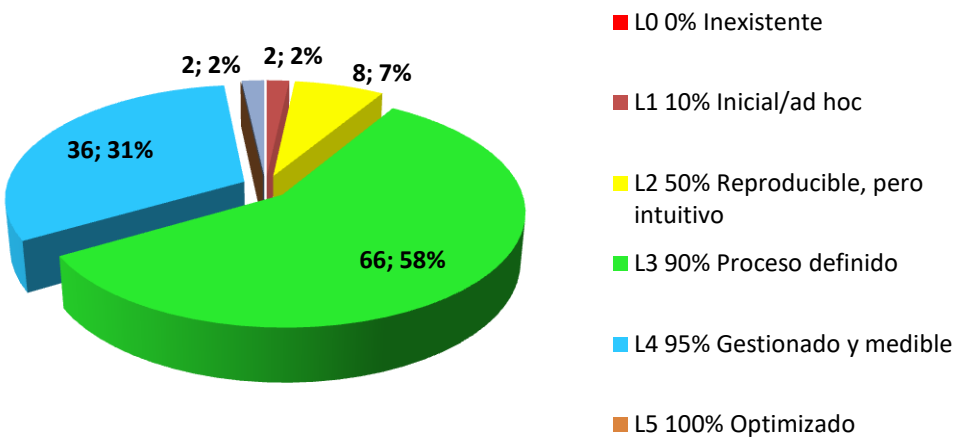

Fig. 10: Niveles de madurez de los controles de seguridad

6.2.3 CONCLUSIONES DE LA EVALUACIÓN

Se puede concluir que la organización tiene implementado un Sistema de Gestión de Seguridad de la Información, ya que la organización se encuentra mayormente en un nivel de madurez gestionado y medible (55%). Con respecto a la evaluación de madurez de los controles implantados de la ISO 27002, se concluye que se tienen mayoritariamente los procesos definidos (58%). A continuación, se muestra el resumen:

ISO 27001			
Nivel	**Efectividad**	**Significado**	**Nº de Controles**
L0	0%	Inexistente	0
L1	10%	Inicial/ad hoc	0
L2	50%	Reproducible, pero intuitivo	2
L3	90%	Proceso definido	7
L4	95%	Gestionado y medible	12
L5	100%	Optimizado	1
ISO 27002			
Nivel	**Efectividad**	**Significado**	**Nº de Controles**
L0	0%	Inexistente	0
L1	10%	Inicial/ad hoc	2
L2	50%	Reproducible, pero intuitivo	8
L3	90%	Proceso definido	66
L4	95%	Gestionado y medible	36
L5	100%	Optimizado	0
N/A			2

7. RESUMEN EJECUTIVO Y CONCLUSIONES

El presente trabajo se ha enmarcado en el desarrollo de un Plan Director de Seguridad para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2015. La organización analizada ha sido una asegurada cuya motivación principal para gestionar la seguridad de la información en su organización ha sido perseguir un servicio de alta calidad, mejorando principalmente el servicio de call center, asegurar la seguridad de la información dentro de sus procesos, dar respuesta a las demandas de seguridad que sus clientes y activos requería, y poder adaptarse a las amenazas que se presentan y a los nuevos requerimientos que el desarrollo legislativo está imponiendo con respeto a la protección de datos de carácter personal.

Cabe mencionar que este trabajo puede ser tomado como referencia para cualquier empresa que quiera gestionar la seguridad de la información y valore externalizar ciertos servicios para prestar una mejor calidad de los mismos, ya que están en pleno crecimiento como es el caso de la empresa expuesta y sus riesgos podrían aumentar.

Para ello, la Dirección ha tomado la decisión de implementar un SGSI con la ayuda de una consultora externa y poder ser conocedora de los principales riesgos y amenazas a los que están expuestos para poder ser gestionados y tratados, y alcanzar mayor efectividad en dicha gestión mediante la mejora continua del SGSI.

Las fases de proyecto que se han llevado a cabo dentro de la empresa han sido las siguientes:

- Se ha realizado un análisis diferencial respecto a la ISO/IEC 27001 y 27002, para conocer el estado actual de la organización en materia de seguridad de la información.
- Se ha creado un sistema de gestión documental para el correcto seguimiento, implementación y gestión del SGSI. En él se encuentran los principales documentos con los que debe contar un SGSI:

    - Política de Seguridad de la Información que expone el debido cumplimiento en seguridad que tiene que ser llevado a cabo por el personal ligado a la organización.
    - Asignación clara de roles y responsabilidades en la organización para la correcta gestión de la seguridad de la información.
    - Análisis y gestión de riesgos que se lleva a cabo en la organización, junto con la Declaración de Aplicabilidad de controles de seguridad.
    - Plan de mejoras de la seguridad de la información e implantación de controles.

- Procedimiento de auditorías para evaluar el estado de la organización en materia de seguridad.

Con el SGSI implementado, se han desarrollado, divulgado y publicado procedimientos para lograr disminuir las amenazas que han salido con mayor probabilidad de ocurrencia que pueden sufrir los activos, que eran el número de errores de los usuarios, errores de mantenimiento y actualización de equipos, ingeniería social, manipulación de los equipos y uso no previsto. En esta dirección se suman los planes de concienciación en seguridad de la información y formación en el uso de herramientas.

También se ha tratado los activos con mayor riesgo, principalmente el CPD, sus servidores e instalaciones, mediante proyectos de mejora para el mismo, el servicio de call center, mediante la externalización del mismo lo cual ha hecho que se preste un servicio de mayor calidad, además de proponer un Plan de Continuidad de Negocio que se hace necesario para asegurar la disponibilidad y continuidad del servicio.

Finalmente, una vez acabada la implementación del SGSI, a falta de terminar uno de sus proyectos propuestos, el Plan de Continuidad de Negocio, se ha realizado una auditoría interna de cumplimiento para evaluar si se están llevando a cabo los requisitos y controles establecidos en las normas tomadas como referencia. Dicha auditoría ha dado como resultado satisfactorio, pero se deben llevar a cabo las recomendaciones dadas para resolver los hallazgos encontrados.

En conclusión, la implementación del SGSI y los principales proyectos de mejora propuestos han hecho que la organización tenga gestionados los principales riesgos no asumidos a los que está sometida la organización, pero dicho plan de proyectos tiene que mejorar en el futuro y alimentarse con más acciones correctivas para llegar a una adecuada gestión de todos los riesgos, produciéndose así una mejora continuada del SGSI implantado.

8. ANEXO

Se adjuntan con este trabajo los siguientes documentos:

- SI-PO-Política de Seguridad de la Información-v.01.pdf
- SI-PRO-Gestión de Roles y Responsabilidades-v.01.pdf
- SI-PRO-Gestión de los Indicadores-v.01.pdf
- SI-PRO-Procedimiento de Revisión por la Dirección-v.01.pdf
- SI-PRO-Procedimiento de Auditorías Internas-v.01.pdf
- SI-CN-PRO-Procedimiento de Uso Aceptable de los Activos-v.01.pdf
- SI-AI-Informe de Auditoría Interna-v.01.pdf
- Cálculos_AR.xlsx
- Presentación de inicio y concienciación en seguridad para la Dirección_v0.11.ppt
- Resumen Estado de los Proyectos de Mejora_v0.1
- Resumen Ejecutivo del Plan_v0.1.ppt
- DefensaTFM-Presentación del Proyecto_V0.1.ppt

9. BIBLIOGRAFÍA

[1] https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4464-ataque-masivo-de-ransomware-que-afecta-a-un-elevado-numero-de-organizaciones-espanolas.html

[2] PWC, *The Global State of Information Security Survey 2017*, http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/assets/gsiss-report-cybersecurity-privacy-possibilities.pdf

[3] ISO/IEC 27002:2013 – Tecnologías de la Información-Técnicas de seguridad-Código de prácticas para los controles de Seguridad de la Información https://www.iso.org/standard/54533.html

[4] ISO/IEC 27001:2015 – Tecnología de la Información-Técnicas de Seguridad- Sistemas de Gestión de Seguridad de la Información - Requerimientos https://www.iso.org/standard/54534.html

[5] Documentación sobre SGSI: Guía de apoyo de SGSI de INCIBE https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

[6] https://www.securityartwork.es/2011/01/12/medicion-de-un-sgsi-disenando-el-cuadro-de-mandos/

[7] MAGERIT – Versión 3.0. Metodología De Análisis y Gestión De Riesgos De Los Sistemas De Información. Libro I - Método. Pág. 6, M. Amutio, J. Candau y J.Antonio Mañas. Descarga: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html#.W_AA8JNKjIU

[8] MAGERIT – Versión 3.0. Metodología De Análisis y Gestión De Riesgos De Los Sistemas De Información. Libro II – Catálogo de elementos. M. Amutio, J. Candau y J.Antonio Mañas.

[9] MAGERIT – Versión 3.0. Metodología De Análisis y Gestión De Riesgos De Los Sistemas De Información. Libro III – Guía de Técnicas. M. Amutio, J. Candau y J.Antonio Mañas.

[10] Guía de Seguridad de las TIC CCN-STIC 470, PILAR – Manual de Usuario v7.1, Centro Criptológico Nacional, Mayo 2018. Descarga: https://www.ccn-cert.cni.es/series-ccn-

stic/guias-de-acceso-publico-ccn-stic/2841-ccn-stic-470i1-pilar-manual-de-usuario-v7-1/file.html

[11] MAGERIT – Versión 3.0. Metodología De Análisis y Gestión De Riesgos De Los Sistemas De Información. Libro II – Catálogo de elementos. Pág. 7-13, M. Amutio, J. Candau y J.Antonio Mañas.

Documentación adicional de apoyo para la elaboración de este Trabajo Fin de Máster:

- RD 3/2010 Esquema Nacional de Seguridad (ENS): https://administracionelectronica.gob.es/ctt/ens/descargas#.W-c9BZNKjIU

- Esquema Nacional de Seguridad –Métricas e indicadores: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/525-ccn-stic-815-indicadores-y-metricas-en-el-ens/file.html

- https://www.incibe.es/protege-tu-empresa

- Material docente de las asignaturas "*Sistema de Gestión de la Seguridad de la Información"* y *"Auditoría Técnica"* de la UOC.